A Semantics for Web Services Authentication

Karthikeyan Bhargavan   Cédric Fournet
Andrew D. Gordon

February 2004

Technical Report
MSR–TR–2003–83

Microsoft Research
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

A shortened version of this paper appears in the proceedings of the *31st Annual ACM SIGPLAN–SIGACT Symposium on Principles of Programming Languages*, Venice, January 14–16, 2004.

A Semantics for Web Services Authentication

Karthikeyan Bhargavan Cédric Fournet Andrew D. Gordon

February 2004

Abstract

We consider the problem of specifying and verifying cryptographic security protocols for XML web services. The security specification WS-Security describes a range of XML security tokens, such as username tokens, public-key certificates, and digital signatures, amounting to a flexible vocabulary for expressing protocols. To describe the syntax of these tokens, we extend the usual XML data model with symbolic representations of cryptographic values. We use predicates on this data model to describe the semantics of security tokens and of sample protocols distributed with the Microsoft WSE implementation of WS-Security. By embedding our data model within Abadi and Fournet's applied pi calculus, we formulate and prove security properties with respect to the standard Dolev-Yao threat model. Moreover, we informally discuss issues not addressed by the formal model. To the best of our knowledge, this is the first approach to the specification and verification of security protocols based on a faithful account of the XML wire format.

Contents

1 Motivations and Outline

Over the past few years, a growing list of specifications has been defining aspects of XML web services. Security is a serious concern and is addressed, in particular, by the recent WS-Security specification [3, 15]. This specification provides an XML vocabulary for designing cryptographic protocols, is widely implemented, and is undergoing standardization at OASIS [31] under the name Soap Message Security. Still, it provides no formal basis for stating security goals or reasoning about correctness. The trouble is, new cryptographic protocols are often flawed, XML or no XML.

Meanwhile, there has been a sustained and successful effort to develop formalisms for expressing and verifying cryptographic protocols ([6, 10, 11, 21, 24, 26, 34, 38] etc). Formal methods can verify various security properties against a standard threat model based on an opponent able to monitor and manipulate messages sent over the network. Such verifications are typically of abstract versions of protocols, expressed using fixed, high-level, ad hoc message formats, rather than the standard XML syntax for ordered trees with pointers.

This paper brings these developments together. We introduce a language-based model for XML security protocols, and we establish process calculus techniques for verifying authentication properties for a wide class of WS-Security protocols.

1.1 Background: Web Services Security

Web services [40] are a distributed systems technology based on network endpoints exchanging SOAP [7] envelopes—XML documents with a mandatory `Body` element containing a request, response, or fault element, together with an optional `Header` element containing routing or security information. SOAP allows for network intermediaries—such as routers or firewalls—to process an envelope, by adding or modifying headers. Examples of web services include Internet-based services for ordering goods or invoking search engines, and intranet-based services for linking enterprise applications.

A common technique for securing SOAP exchanges is to rely on a lower-level secure tunnel between the endpoints, typically an SSL connection. This works well in many situations, but has the usual disadvantages of transport-level security: the secrecy or integrity of messages can be guaranteed while in the tunnel, but not subsequently in files or databases, and they may not match the security requirements of the application. Pragmatically, client authentication is often performed by the application rather than by SSL. Besides, SSL does not fit SOAP's message-based architecture: intermediaries cannot see the contents of the tunnel, and so cannot route or filter messages.

To better support end-to-end security [35], WS-Security defines how to sign or encrypt SOAP messages without relying on a secure transport. A central—but informal—abstraction is the *security token*, which covers data making security claims, such as user identifiers, cryptographic keys, or certificates. WS-Security provides a precise syntax for multiple token formats, such as XML username tokens and XML-encoded binary tokens conveying X.509 public-key certificates or symmetric keys. It also specifies syntax for applying encryption and signature to selected elements of SOAP messages. Like many traditional protocol specifications, WS-Security details message formats—such as the names of XML tags—rather than security goals and their enforcement, thereby focusing on interoperability rather than security. Although it gives a syntax for a broad range of protocols, WS-Security also emphasizes flexibility, and does not define any particular protocol. As a result, for each given WS-Security compliant protocol, security goals still have to be carefully specified and validated.

1.2 Background: Security Protocol Verification

This paper addresses authentication properties of XML-based security protocols against a standard threat model: an opponent able to read, replay, redirect, and transform messages, but who cannot simply guess secrets. Needham and Schroeder describe such an opponent in their pioneering work on cryptographic protocols [32]. The first formalization was by Dolev and Yao [17]. A great many formal methods have been deployed to verify protocols against this threat model, with particular progress in the past few years.

This paper uses Abadi and Fournet's applied pi calculus [1, 20] as the underlying specification language for protocols, and relies on proof techniques from concurrency theory. In this approach, the opponent is simply an arbitrary context within the calculus; the scoping rules of the pi calculus ensure that the opponent cannot learn names representing secrets such as the passwords of protocol participants.

We formalize authentication properties using standard correspondence assertions [41], as embedded within the pi calculus by Gordon and Jeffrey [21]. These assertions are based on two kinds of events, which can be thought of as logfile entries by protocol participants. A begin-event marks the initiation of a run of a protocol, while an end-event marks the commitment that a run has completed. Events record data identifying the run, such as the names of the client and server, message identifier, and payload. A protocol is safe if in every run, every end-event corresponds to a previous begin-event with the same event record. Moreover, a protocol is robustly safe if it is safe in the presence of an arbitrary opponent process. Robust safety establishes message authentication, and rules out a range of attacks.

1.3 This Paper

We tackle the problem of formal reasoning about XML-encoded cryptographic protocols. The interest and novelty in this problem arises not from the XML syntax itself, but from the need to model low-level detail, in particular, the flexibility and hierarchical structure of XML signatures [19], designed to tolerate changes to the headers of a SOAP message over its lifetime.

We base our approach on three formalisms: a symbolic syntax for XML with cryptography and a predicate language for defining acceptable messages—both defined in Section 2—and a specialized version of the applied pi calculus. We explain the purpose of each of these in turn.

First, to represent XML messages with embedded cryptography, we enrich the standard XML data model with an abstract syntax for embedded byte arrays and cryptographic functions. Formally, we define a many-sorted algebra with sorts for the usual constructs of XML—strings, attributes, and so on—plus a new sort of symbolic byte arrays, in the style of Dolev and Yao, to represent cryptographic materials embedded in XML.

Second, to define the semantics of security tokens and validity conditions on messages, we introduce a Prolog-like language of predicates on XML data. By insisting on fidelity to the low-level XML format, we are confronted with the difficulty of defining rather intricate conditions of message acceptability, and hence we need some language of predicates on XML. It may be possible to extend some standard type system or query language for XML (such as DTDs, XML Schema, or XPath) to express conditions on cryptographic values. Instead, for the sake of simplicity and being self-contained, we rely on a fairly standard Horn-clause logic.

Third, to describe complete protocols, we embed these messages and predicates within the applied pi calculus. We state and prove protocol properties against a large class of contexts representing attackers. Applied pi is parameterized in general by an arbitrary equational theory of terms, which we specialize to our data model for XML with cryptography. We obtain a calculus expressive enough to implement our predicates, and to describe complex protocol configurations.

In Section 3, given these notations, we formalize the security goals and message formats of a series of sample protocols. These protocols illustrate a range of WS-Security concepts including message identifiers, password digests, username tokens, X.509 public-key certificates, XML signatures based on both password-derived keys and certificates, and processing by SOAP intermediaries as well as end-points. For each protocol, we give predicates describing acceptable messages, and state authentication goals using the usual message-sequence notation. WS-Security itself defines a formal syntax for messages, but gives only an informal account of the security checks performed by compliant implementations, as each token is processed in the SOAP protocol stack. Through formalizing the series of protocols, we accumulate a collection of re-usable predicates reflecting the semantics of these tokens. Hence, we obtain a first formal semantics for a significant fragment of WS-Security.

In Section 4, we formalize the message-sequence notation within the applied pi calculus so as to verify our authentication goals. We explain the structure of the proof of three of the sample protocols from Section 3. The proofs are compositional, and rely on identifying a "trusted computing base" embodying the essential checks underlying the protocol.

In Section 5, we conclude, and discuss related and future work.

Appendix A is a brief introduction to the applied pi calculus. Appendix B contains additional proofs. Appendix C lists the namespaces for all XML element and attribute names used in the paper. Appendix D provides sample SOAP messages obtained experimentally for the protocols of Section 3. A portion of this report is published as a conference paper [5].

1.4 Contributions

In summary, we make three main contributions:

(1) A new data model and predicate language for describing XML-level cryptographic protocols.

Fidelity to the detailed messaging format enables us to address its subtleties, such as the interpretation of compound signatures.

(2) A collection of predicates defining a semantics for the security tokens of WS-Security and related specifications.

We cover only a substantial fragment of WS-Security, but our semantics does establish the feasibility of applying our formal developments to a large class of protocols.

(3) Proofs for a series of concrete protocols drawn from the WSE 1.0 distribution.

At an abstract level, the protocols we consider are quite simple. Still, we have encountered vulnerabilities to XML rewriting attacks in implementations of these conceptually simple protocols. So it is worth establishing correctness at this level, and indeed the formal Dolev-Yao properties are non-trivial.

2 Symbolic Cryptography in XML

The core of our data model—or abstract syntax—for XML trees is adapted from Siméon and Wadler's grammar for XML [37].

XML Data Model: Standard Core

Tag	::= `anyLegalXmlName`	element or attribute name
str:string	::= `any legal XML string`	XML string
a:att	::= *Tag*=`"`*str*`"`	*Tag*-attribute
as:atts	::= *a as* | ϵ	attribute sequence
i:item	::= *Elem* | *str*	item
is:items	::= *i is* | ϵ	item sequence
Elem	::= `<`*Tag as*`>`*is*`</`*Tag*`>`	*Tag*-element

Our data model represents valid, parsed XML. It resembles the XML infoset recommendation [12] but with some differences. For the sake of clarity, we completely suppress information about XML namespaces, and the document `<?xml ...>` directive. As a minor technical convenience, we model an element's attributes as an ordered sequence rather than a set. (This also reflects the capability of an attacker to observe ordering information.)

Our syntax is intentionally close to the standard XML wire format, but for brevity we rely on three notational conventions. First, although formally an element's attributes *as* and body *is* are recursively defined lists, we typically use a standard tuple notation for fixed-length sequences. Second, instead of writing an element `<Envelope></Envelope>`, say, in full, we drop the tag from the closing bracket, and simply write `<Envelope></>`. Third, when writing an element that spans several lines, we rely on indentation (as in Haskell or Python) to delimit the body, and so omit the closing bracket. So, by convention,

```
<Envelope>
  <Header></>
  <Body></>
```

is short for `<Envelope><Header></Header><Body></Body></Envelope>`.

Conventions for Sequences, for Closing and Indenting Elements:

$a_1 \ \ldots \ a_m \triangleq a_1 \ (\ldots \ (a_m \ \epsilon)) : \mathsf{atts}$ for $m \geq 0$; similarly for items.

$\texttt{<}\mathit{Tag}\ \mathit{as}\texttt{>}\mathit{is}\texttt{</>} \triangleq \texttt{<}\mathit{Tag}\ \mathit{as}\texttt{>}\mathit{is}\texttt{</}\mathit{Tag}\texttt{>}$

$$\left.\begin{array}{l}\texttt{<}\mathit{Tag}\ \mathit{as}\texttt{>}\\ \quad i_1\\ \quad \vdots\\ \quad i_m\end{array}\right\} \triangleq \texttt{<}\mathit{Tag}\ \mathit{as}\texttt{>}i_1 \cdots i_m\texttt{</>}$$

Formally, our data model is a many-sorted algebra, based on the sorts string, att, atts, item, items, plus a sort bytes for binary data. We embed this algebra within the applied pi calculus as described in Section 4. The complete algebra is given by the "XML Data Model" table above plus two more below.

We need the following general definitions. We let T, U, V range over terms of arbitrary sort in the algebra, and write $T : \mathsf{string}$, for example, to mean that T belongs to the sort string. Throughout we assume that terms, predicates, and equations are well-sorted, but for the sake of brevity keep the details implicit. In addition to the syntax defined in this section, terms include sorted variables, $x, y, z, \ldots$, and so on. We let $\mathit{fv}(T)$ be the set of variables occurring in a term T. We say a term T is *closed* if and only if $\mathit{fv}(T) = \varnothing$. Otherwise, we say the term is *open*—an open term represents a closed term with some undetermined subterms, represented by the variables. We let $\widetilde{V}$ range over vectors $V_1, \ldots, V_m$ of terms, and similarly $\widetilde{x}$ ranges over vectors $x_1, \ldots, x_m$ of variables. We often treat such vectors as sets. We let σ range over parallel substitutions $\{\widetilde{x} = \widetilde{V}\}$ of the terms $\widetilde{V}$ for the variables $\widetilde{x}$, and we define $\mathit{dom}(\{\widetilde{x} = \widetilde{V}\}) \triangleq \{\widetilde{x}\}$. We say that a substitution σ is *closed* if and only if $\sigma(x)$ is a closed term for each $x \in \mathit{dom}(\sigma)$.

Next, we supplement the core data model with a symbolic representation of cryptography and related operations. We introduce a sort bytes representing byte arrays, and extend string with Base64-encoded arrays ($\mathsf{base64}(x)$). We assume there is an infinite set of atomic, abstract *names*, ranged over by s. Each name is either of sort bytes or string. We use these names to represent arbitrary, unstructured cryptographic materials such as passwords and keys. We let $\mathit{fn}(T)$ be the set of names occurring in a term T.

XML Data Model: Byte Arrays, Symbolic Cryptography

x: bytes ::=	byte array (not itself XML)
s	abstract name (key, nonce)
concat(x_1, x_2 : bytes)	array concatenation
c14n(i: item)	canonical bytes of an item
utf8(str: string)	UTF8 representation of strings
sha1(x: bytes)	cryptographic digest
p-sha1(pwd: string, $salt$: bytes)	key from salted password
hmac-sha1(key, x: bytes)	keyed hash
pk(k_{priv} : bytes)	map from private to public key
rsa-sha1(x, k_{priv} : bytes)	public key signature
x509(s_r : bytes, u : string, a : string, k_{pub} : bytes)	X.509 certificate
str: string ::=	XML string
s	abstract name (password)
base64(x: bytes)	Base64-encoding of byte array
principal(pwd: string)	map from password to principal

While the cryptographic functions presented here are all present in the WS-Security specification, the exact choice of primitives is a little arbitrary; we include enough operations here for the protocols of Section 3. The term concat(x_1, x_2) represents the concatenation of the two arrays x_1 and x_2. The term c14n(i) represents the array obtained by canonicalizing the XML represented by i, according to some standard algorithm [8, 9]. (In fact, for our purposes, c14n is simply a way of symbolically treating an XML item as a byte array; our c14n does not sort attribute lists, for example.) The term utf8(str) represents the UTF8 encoding of the XML string str. The term sha1(x) represents the one-way SHA1 hash of the x array. The term p-sha1(pwd,$salt$) represents a key obtained by hashing the pwd password and the $salt$ array [16]. The term hmac-sha1(key, x) represents a keyed hash of the x array using the key array as the key [25]. The term pk(k_{priv}) represents the public key associated with a private signing key k_{priv}. The term rsa-sha1(x, k_{priv}) is a public-key signature of x under the private key k_{priv} [23]. The term x509(s_r, u, a, k) represents a basic X.509 public-key certificate, where s_r is the private signing key of the certifier and u, a, k are the signed user name, algorithm, and key for a given principal. (Such binary certificates can be embedded as XML items; they are used here to carry public keys for the asymmetric signing algorithm rsa-sha1.) Finally, the term principal(pwd) is used to represent a database of user names associated with secrets, such as passwords, and is explained in Section 3.2.

Our threat model is that SOAP messages may be intercepted, decomposed, modified, assembled, and replayed by the attacker [17, 32]. The following selector functions and inverses symbolically represent the ability of the attacker to decompose messages. It is deliberate that there are no inverses for the three hash functions (sha1, p-sha1, and hmac-sha1), and for the public-key (pk) and user name (principal) maps; the attacker cannot reverse these one-way functions.

XML Data Model: Selectors and Inverses

x: bytes ::=	byte array
fst(x: bytes)	left part of concat
snd(x: bytes)	right part of concat
i-base64(str: string)	inverse of base64
x509-key($cert$: bytes)	public key in X.509 certificate
check-x509($cert, k_r$: bytes)	X.509 certificate verification
check-rsa-sha1(x, sig, k_{pub}: bytes)	public key verification
str: string ::=	XML string
Tag.parm(a: att)	string param of a Tag-attribute
i-utf8(x: bytes)	inverse of utf8
x509-user($cert$: bytes)	name in X.509 certificate
x509-alg($cert$: bytes)	algorithm in X.509 certificate
a: att ::=	attribute
hd(as: atts)	head of a sequence
as: atts ::=	attributes
Tag.att(i: item)	attributes of a Tag-element
tl(as: atts)	tail of a sequence
i: item ::=	item
hd(is: items)	head of a sequence
i-c14n(x: bytes)	inverse of c14n
is: items ::=	items
Tag.body(i: item)	body of a Tag-element
tl(is: items)	tail of a sequence

Most of these selectors are straightforward inverses with single arguments. The two exceptions are check-x509 and check-rsa-sha1. The term check-x509($cert, k_r$) checks that the certificate $cert$ is signed with a private key associated with the public key k_r, and yields k_r if this succeeds. The term check-rsa-sha1(x, sig, k_{pub}) checks that sig is the rsa-sha1 signature of x under the private key corresponding to the public key k_{pub} and yields k_{pub} if this succeeds. (Some of the inverses, such as the functions fst and snd, would be impossible to implement in general, and we do not rely on them to program compliant principals; they exist to represent the possibility of the attacker correctly guessing, for example, how to divide an array obtained by concatenation into its original two halves.)

We represent evaluation of selectors and inverses by an equivalence, $U = V$, the least sort-respecting congruence induced by the following axioms.

Equivalence of Terms of the Data Model: $U = V$

hd($a\ as$) $= a$	tl($a\ as$) $= as$
hd($i\ is$) $= i$	tl($i\ is$) $= is$
Tag.att(<$Tag\ as$>is</>) $= as$	i-base64(base64(x)) $= x$
Tag.body(<$Tag\ as$>is</>) $= is$	i-utf8(utf8(str)) $= str$
Tag.parm(Tag="str") $= str$	i-c14n(c14n(i)) $= i$
fst(concat(x_1, x_2)) $= x_1$	snd(concat(x_1, x_2)) $= x_2$

$\mathsf{x509\text{-}user}(\mathsf{x509}(s_r, u, a, k)) = u$ $\quad\quad$ $\mathsf{x509\text{-}alg}(\mathsf{x509}(s_r, u, a, k)) = a$
$\mathsf{x509\text{-}key}(\mathsf{x509}(s_r, u, a, k)) = k$
$\mathsf{check\text{-}x509}(\mathsf{x509}(s_r, u, a, k), \mathsf{pk}(s_r)) = \mathsf{pk}(s_r)$
$\mathsf{check\text{-}rsa\text{-}sha1}(x, \mathsf{rsa\text{-}sha1}(x, k_{priv}), \mathsf{pk}(k_{priv})) = \mathsf{pk}(k_{priv})$

In the absence of additional equivalences between terms, we implicitly assume that our cryptographic operations have no additional interactions. For instance, the hash functions sha1, p-sha1, hmac-sha1, and rsa-sha1 are independent here. This can be informally checked from their cryptographic specifications [18, 16, 25, 23], or modelled as a refinement of the term equivalence, as in [1].

We end this section by defining a logical notation for predicates on XML terms. Formally, we present a Horn logic over our many-sorted algebra, with primitive formulas for equality and list membership, but no recursively-defined predicates. Our notation is simple, and suffices for reasoning about security; other languages feature more expressive pattern-matching for XML, but their semantics would be harder to formalize.

We assume there is a fixed, finite set of *predicates*, ranged over by p. For each predicate p, we assume there is a single definition $p(\widetilde{x})$:- $\Phi_1 \vee \cdots \vee \Phi_m$, where each Φ_i is a *formula*, and $m > 0$. (When $m > 1$, we usually present each clause $p(\widetilde{x})$:- Φ_i separately, in the style of Prolog.) Next, we define the syntax of formulas.

Syntax of Formulas and Predicate Definitions:

$\Phi ::=$	formula
$\quad V = T$	term comparison
$\quad U \in V$	list membership
$\quad p(\widetilde{V})$	predicate instance
$\quad \Phi_1, \Phi_2$	conjunction
$p(\widetilde{x})$:- $\Phi_1 \vee \cdots \vee \Phi_m$	definition of predicate p with $m > 0$

We assume that formulas are well-sorted according to the following rules: in $V = T$ both terms belong to the same sort; in $U \in V$ either U : item and V : items or U : att and V : atts; in $p(\widetilde{V})$ when $p(\widetilde{x})$:- $\Phi_1 \vee \cdots \vee \Phi_m$, the length and sorts of $\widetilde{V}$ match the length and sorts of $\widetilde{x}$.

Let p contribute to q if and only if an instance $p(\widetilde{V})$ occurs in one of the disjuncts defining q. We stipulate that this relation is well-founded, to avoid recursively-defined predicates. We let $fv(\Phi)$ be the free variables of all the terms occurring in Φ, and in particular, $fv(p(V_1, \ldots, V_m)) \triangleq fv(V_1) \cup \cdots \cup fv(V_m)$. In any clause $p(\widetilde{x})$:- Φ, we say that each $z \in fv(\Phi) \setminus \widetilde{x}$ is a *local variable*. By convention, each occurrence in a clause of the wildcard symbol _ is short for the only occurrence of a fresh local variable. Local variables are existentially quantified in our semantics; we identify clauses up to the consistent renaming of local variables.

Semantics of Formulas: $\models \Phi$ **where** $fv(\Phi) = \varnothing$

$\models V = T \triangleq (V = T)$
$\models U \in V \triangleq (V = U_1 \ \ldots \ U_i \, U \, V')$
  for some $U_1, \ldots, U_i, V'$, with $i \geq 0$
$\models p(\widetilde{V}) \triangleq \ \models \Phi_i\{\widetilde{x} = \widetilde{V}\}\{\widetilde{z} = \widetilde{U}\}$
  for some $i \in 1..m$ and closed terms $\widetilde{U}$
  where $p(\widetilde{x})$ `:-` $\Phi_1 \vee \cdots \vee \Phi_m$ and $\widetilde{z} = fv(\Phi_i) \setminus \widetilde{x}$
$\models \Phi_1, \Phi_2 \triangleq \ \models \Phi_1$ and $\models \Phi_2$

For open formulas, we introduce notions of validity and logical equivalence.

Validity, Logical Equivalence of Formulas:

A formula Φ is *valid* when, for all substitutions σ such that $\Phi\sigma$ is closed, $\models \Phi\sigma$. Two formulas Φ, Φ' are *logically equivalent* when, for all substitutions σ such that $\Phi\sigma$ and $\Phi'\sigma$ are closed, $\models \Phi\sigma$ iff $\models \Phi'\sigma$.

3 Example Protocols

This section describes some WS-Security protocols, whose goal is to authenticate access to a basic web service. We first present a typical (unauthenticated) web service, then successively refine it by introducing password-based digests, signatures, X.509 certificates, and a firewall intermediary. The first four protocols are taken from the samples provided with WSE 1.0 [29]; we used the actual SOAP messages produced by this implementation to experimentally validate our model. (Appendix D includes sample messages produced by WSE.)

3.1 An (Unauthenticated) Web Service

We consider a typical e-commerce website application where customers can browse and purchase items [28]. The orders are stored on a database server, and can be retrieved and viewed on later visits. For security, customers are required to login, with username and password, before placing and retrieving orders. In addition to the standard website interface, the server provides a SOAP web service *GetOrder* that a customer may invoke to retrieve their order in XML format, to save it as a receipt, for instance. Our aim is to provide the same level of security for this web service as the website login.

A call to *GetOrder* consists of a SOAP request and a SOAP response. We introduce predicates to describe these messages. As a first example, a valid SOAP message is an XML `Envelope`, containing a `Header` and a `Body`. The predicate $hasBody(e, b)$ below means b is the body of envelope e (the wildcard _ matches anything):

```
hasBody(e : item, b : item) :-
  e = <Envelope><Header>_</>b</>,
  b = <Body _>_</>.
```

The SOAP request for *GetOrder* is an envelope, where the body encodes the parameters of the call. The resulting SOAP response has a body containing the order, in XML:

```
isGetOrder(b : item, OrderId : string) :-
  b = <Body _>
        <GetOrder>
          <orderId>OrderId</>

isGetOrderResponse(b : item, OrderId : string, u : string) :-
  b = <Body _>
        <GetOrderResponse>
          <orderId>OrderId</>
          <date>_</>
          <userId>u</>
          _
```

We suppose there is a single server, identified by the URL S, hosting the *GetOrder* web service, identified by the URI W, and multiple client computers that may connect to S on behalf of users. Here is a protocol for a client computer, identified by its IP address I, to request information about order number *OrderId* from the web service W on server S, on behalf of a human user u.

Message 1:	$I \to S, W \quad e$
	where $hasBody(e, b)$, $isGetOrder(b, OrderId)$
Message 2:	$S \to I \quad e'$
	where $hasBody(e', b')$,
	and $isGetOrderResponse(b', OrderId, u')$

- Message 1 is an HTTP POST request to the URL S, with an HTTP header `SOAPAction:` W, and with the SOAP envelope e as its content. The predicates $hasBody(e, b)$ and $isGetOrder(b, OrderId)$ specify the behaviour of both client and server: that is, a client will only send Message 1, and a server will only accept it, if the message e is a suitably formatted request for some order *OrderId*. We implicitly specify that if the server receives a message that does not satisfy these predicates, it will reject the message.

- Message 2 is the HTTP response, containing the SOAP envelope e'. The predicates $hasBody(e', b')$ and $isGetOrderResponse(b', OrderId, u')$ constrain the server to send a reply that concerns the order *OrderId* requested in Message 1. In this first protocol, the user u whose client computer sends the request need not be the same as the user u' who is associated with the order.

It is not a goal here to fully specify the correct behaviour of either client or server. We are only concerned about security properties, and authentication in particular, and suppress other information. For example, we suppress the rest of the response, which includes details such as the credit card type, number and expiration date, billing and shipping addresses, and the sequence of line items in the order.

Our predicates express constraints on messages sent and received by compliant implementations of our protocols. On the sender side, they express post-conditions for every outgoing message. (The fact that these conditions do not fully determine the envelope yields functional flexibility.) On the receiver side, they express pre-conditions that must be checked before incoming messages are processed. (They do not specify a particular order for the checks, but still provide enough details to review an implementation.) In the presence of an active attacker, it is essential that the receiver dynamically check these conditions, even if the sender enforces them.

Our first protocol offers no protection against active attacks, since any well-formed envelope is accepted by the server. Next, we consider more effective checks.

3.2 Password Digest

Username tokens with a cryptographic digest provide a first, basic mechanism for authenticating web service requests. Such tokens include a username identity u, together with a digest of a password and a fresh timestamp. We assume that each password pwd_u is a shared, unguessable secret between u and S, so that only u (or S, in principle) can generate a valid digest—this hypothesis excludes dictionary attacks, for instance. To justify this assumption, passwords need to be strong cryptographic secrets; one might also modify the protocol to encrypt the digest of a weak password, but we do not pursue this alternative. Moreover, as in other applications of the applied pi calculus, we abstractly relate the password and the user using the special one-way function $\mathsf{principal}$ from passwords to users: we let u stand for $\mathsf{principal}(pwd_u)$.

To model this protocol, we develop predicates for describing WS-Security headers and embedded username tokens. Our predicate definitions are not specific to this protocol, and can be re-used for any protocol relying on these tokens. First, we define a predicate to extract the security tokens from some security header of the envelope: the predicate $hasSecurityHeader(e, toks)$ means that $toks$ is a sequence of security tokens attached to message e. The first formula in the predicate body extracts the list of headers ($headers : \mathsf{items}$) from the envelope. The second formula, $header \in headers$, requires that $header$ be some member of the header list. The third formula requires that $header$ be a security header, and extracts the security tokens from it.

$$\begin{array}{l} hasSecurityHeader(e : \mathsf{item}, toks : \mathsf{items}) \texttt{ :-} \\ \quad e = \texttt{<Envelope><Header>}headers\texttt{</>\_</>}, \\ \quad header \in headers, \\ \quad header = \texttt{<Security>}toks\texttt{</>}. \end{array}$$

The WS-Security specification allows envelopes to contain multiple `<Security>` elements, possibly containing SOAP `role` attributes, provided each `<Security>`

element in an envelope is targeted at a distinct endpoint or intermediary. For the sake of simplicity, *hasSecurityHeader* ignores `<Security>` elements containing this attribute, and does not check for duplicate `<Security>` elements.

With username tokens, the unique identifier of a message is a pair $(n : \mathsf{bytes}, t : \mathsf{string})$ where n is a nonce—some byte array—and t is a timestamp represented as a string. The predicate $\mathit{isDigestUserToken}(\mathit{tok}, u, \mathit{pwd}, n, t)$ means that tok is a username token for user u with password pwd, identifier (n, t), and a valid digest.

```
isDigestUserToken(tok : item, u, pwd : string, n : bytes, t : string) :-
  tok = <UsernameToken _>
          <Username>u</>
          <Password Type="PasswordDigest">base64(d)</>
          <Nonce>base64(n)</>
          <Created>t</>,
  u = principal(pwd),
  d = sha1(concat(n, concat(utf8(t), utf8(pwd)))).
```

Finally, a top-level authentication predicate, *hasUserTokenDigest*, gathers all the elements checked on envelopes received by the server; $\mathit{hasUserTokenDigest}(e, u, \mathit{pwd}, n, t, b)$ means that the envelope e with body b contains a valid username token for u, pwd, n, t.

```
hasUserTokenDigest(e : item, u, pwd : string,
                          n : bytes, t : string, b : item) :-
  hasSecurityHeader(e, toks),
  utok ∈ toks,
  isDigestUserToken(utok, u, pwd, n, t),
  hasBody(e, b).
```

The following protocol description includes both SOAP messages and additional begin- and end-events, in the style of Woo and Lam [41]. We introduce these events to express the authentication guarantee obtained by the server from running this protocol. (The correspondence between begin- and end-events is sometimes referred to as agreement between running and commit signals, respectively [27].)

```
   Event 1:  I logs <Begin>u n t</>
 Message 1:  I → S, W    e
             where hasUserTokenDigest(e, u, pwd, n, t, b),
             and isGetOrder(b, OrderId)
   Event 2:  S logs <End>u n t</>
 Message 2:  S → I    e′
             where hasBody(e′, b′),
             and isGetOrderResponse(b′, OrderId, u)
```

We interpret events in the abstract log as follows: before issuing a request, the initiator logs its intent as an entry `<Begin>`$u\ n\ t$`</>` that contains the user name u and the message identifier. Conversely, after checking an envelope, the server logs `<End>`$u\ n\ t$`</>` to manifest that it accepts a request with these parameters. In any case, the attacker cannot log entries. Ideally, begin- and end-events should be in direct correspondence, but this is clearly not the case if the attacker can delete, reorder, or replay u's messages. Instead, we have the following correspondence property:

Claim 1 *In the presence of an active Dolev-Yao attacker, if* `<End>`$u\ n\ t$`</>` *is logged by S, then* `<Begin>`$u\ n\ t$`</>` *has been logged by I.*

This is a fairly weak authentication property, which can be read as "if S accepts a request from u, then u recently sent some request." The two requests are not necessarily the same: for instance, an active attacker can intercept the envelope, modify its body, and pass it to the server. In many settings, it may be suitable to have a stronger correspondence between u and S's actions, for example between entries `<Begin>`$u\ S\ W\ n\ t\ OrderId$`</>` and `<End>`$u\ S\ W\ n\ t\ OrderId$`</>`.

Although the password digest is optional in WS-Security username tokens, our claim would clearly not hold if the server accepted tokens without checking the digest, since the attacker could then forge a message with any identifier (n, t) irrespective of the user's requests.

In itself, our protocol does not eliminate replays. (Technically, our correspondence assertion is non-injective.) However, since the identifier is authenticated, the application can safely use it to filter messages with duplicate or expired username tokens.

3.3 Password-Based Signature

In order to achieve more precise authentication properties under the same assumptions—a shared password between u and S—one can use an XML digital signature on selected elements of the envelope [19]. In addition to the username token, we embed a signature token that signs (for instance) the envelope body, with a signing key derived from the password and the username token.

A hash-based signature of items x_1, ..., x_m using a key k, may be roughly pictured as follows.

```
<Signature>
  <SignedInfo>
    <CanonicalizationMethod Algorithm="... normalization scheme ..."></>
    <SignatureMethod Algorithm="... keyed hash function ..."></>
    <Reference>... hash of x_1 ...</>
    ...
    <Reference>... hash of x_m ...</>
  <SignatureValue>
    ... hash of SignedInfo element with key k ...
```

See Section 4.3 for a full example of a signed envelope. Next, we define the additional predicates needed for our modified protocol, including predicates defining the various parts of a signature.

- $\mathit{isUserTokenKey}(\mathit{tok}, u, \mathit{pwd}, n, t, k)$ means that tok is a username token for user u with password pwd, unique identifier (n, t), and derived key k. The key derivation uses a `p-sha1` keyed hash salted with the message identifier.

- $\mathit{isSigVal}(\mathit{sv}, \mathit{si}, k, a)$ means that sv is the digital signature computed on the item si with key k using algorithm a (which for password-based signatures is `hmac-sha1`).

- $\mathit{ref}(t, r)$ means that the item r is a reference containing the digest of item t. (We use the three wildcards _ to match reference attributes and `Transforms` and `DigestMethod` elements, which are included in references for flexibility, but are irrelevant for security in our setting.)

- $\mathit{isSigInfo}(\mathit{si}, a, x_1, \ldots, x_m)$ means that the signed information si, for signature algorithm a, contains a list of references of which the first m are for the items $x_1, \ldots, x_m$. After these references, si may contain any number of references to other items (represented in the predicate by an _). This flexibility in the predicate enables the client to sign additional items even if not required by the server (to conform to a uniform send policy, for example).

- $\mathit{isSignature}(\mathit{sig}, a, k, x_1, \ldots, x_m)$ means that the signature sig signs $x_1, \ldots, x_m$ with algorithm a and verification key k.

- $\mathit{hasUserSignedBody}(e, u, \mathit{pwd}, n, t, b)$ is the top-level predicate. It means that the envelope e contains a username token for u, pwd, n, t, and that the body b of e is signed by the key derived from the token.

The message exchange is much as in Section 3.2, with two differences: each log entry now contains $u\ n\ t\ \mathit{OrderId}$ instead of just $u\ n\ t$; we use the top-level predicate $\mathit{hasUserSignedBody}(e, u, \mathit{pwd}, n, t, b)$ instead of $\mathit{hasUserTokenDigest}(e, u, \mathit{pwd}, n, t, b)$.

Event 1:	I logs `<Begin>`$u\ n\ t\ \mathit{OrderId}$`</>`
Message 1:	$I \rightarrow S, W \quad e$
	where $\mathit{hasUserSignedBody}(e, u, \mathit{pwd}, n, t, b)$,
	and $\mathit{isGetOrder}(b, \mathit{OrderId})$
Event 2:	S logs `<End>`$u\ n\ t\ \mathit{OrderId}$`</>`
Message 2:	$S \rightarrow I \quad e'$
	where $\mathit{hasBody}(e', b')$,
	and $\mathit{isGetOrderResponse}(b', \mathit{OrderId}, u)$

We obtain a similar, but stronger authentication property:

Claim 2 *In the presence of an active Dolev-Yao attacker, if* `<End>`$u\ n\ t\ \mathit{OrderId}$`</>` *is logged by* S*, then* `<Begin>`$u\ n\ t\ \mathit{OrderId}$`</>` *has been logged by* I*.*

This claim can be read as "if S accepts a request from u, then u recently sent this request." Although only b is signed, the username u and the identifier (n, t) are also authenticated by the signature check. As before, we can rely on (n, t) for replay protection. Since the identifier is now bound to the message, the server can safely use it to filter duplicate or expired messages.

```
$isUserTokenKey(tok : \mathsf{item}, u, pwd : \mathsf{string},$
                                 $n : \mathsf{bytes}, t : \mathsf{string}, k : \mathsf{bytes})$ :-
  $tok =$ <UsernameToken _>
            <Username>$u$</>
            _
            <Nonce>base64($n$)</>
            <Created>$t$</>,
  $u = \mathsf{principal}(pwd)$,
  $k = \mathsf{p\text{-}sha1}(pwd, \mathsf{concat}(n, \mathsf{utf8}(t)))$.

$isSigVal(sv : \mathsf{bytes}, si : \mathsf{item}, k : \mathsf{bytes}, a : \mathsf{string})$ :-
  $a =$ hmac-sha1,
  $sv = \mathsf{hmac\text{-}sha1}(k, \mathsf{c14n}(si))$.

$ref(t : \mathsf{item}, r : \mathsf{item})$ :-
  $r =$ <Reference _>
         _ _ <DigestValue>base64(sha1(c14n($t$)))</>.

                                                    (for each $m \geq 1$)
$isSigInfo(si : \mathsf{item}, a : \mathsf{string}, x_1, \ldots, x_m : \mathsf{item})$ :-
  $si =$ <SignedInfo>
         _ <SignatureMethod Algorithm="$a$"></>
         $r_1 \ \ldots \ r_m$ _,
  $ref(x_1, r_1), \ldots, ref(x_m, r_m)$.

$isSignature(sig : \mathsf{item}, a : \mathsf{string}, k : \mathsf{bytes}, x_1, \ldots, x_m : \mathsf{item})$ :-
  $sig =$ <Signature>$si$ <SignatureValue>base64($sv$)</>_</>,
  $isSigInfo(si, a, x_1, \ldots, x_m)$,
  $isSigVal(sv, si, k, a)$.

$hasUserSignedBody(e : \mathsf{item}, u : \mathsf{string}, pwd : \mathsf{string},$
                                 $n : \mathsf{bytes}, t : \mathsf{string}, b : \mathsf{item})$ :-
  $hasBody(e, b)$,
  $hasSecurityHeader(e, toks)$,
  $utok \in toks$,
  $isUserTokenKey(utok, u, pwd, n, t, k)$,
  $sig \in toks$,
  $isSignature(sig,$ hmac-sha1$, k, b)$.
```

We make two observations concerning these predicates. First, *isUserTokenKey* does not check the presence or validity of the optional username token digest. In fact, checking the password digest would not provide any additional authentication guarantee here. Conversely, its (potential) occurrence in the envelope slightly complicates our proofs in Section 4. Arguably, the initiator should not include both a digest and a signature, since this may facilitate a dictionary attack on the password, unless it does not know which evidence will be considered by the server.

Second, although each reference r typically provides a pointer to the digested element, either as a fragment URI or as an XPath expression, we do not rely on this information in the *ref* predicate. Instead, we check that the actual item we are interested in—the body b—is targeted by the reference. In general, this approach is preferable, since it leaves the resolution of pointers outside the trusted computing base. Otherwise, one should also carefully check that these pointers are well-defined and unambiguous.

Our specification captures the flexibility of WS-Security signatures. The predicates for key derivation (*isUserTokenKey*) are independent from those interpreting the signature. So, we can compose *isSignature* with some other keying material, such as an X.509 certificate. Similarly, we can support additional algorithms for computing the actual signature by adding alternatives to the predicate *isSigVal*—see Section 3.4.

Furthermore, *isSignature* allows additional elements of the message to be signed. Signing the username, nonce, or timestamp elements is not necessary with this particular signing-key derivation, but is harmless, and becomes necessary with other kinds of keys (see Section 3.5). In case there are several actions on the same server, or if the same password is shared with two different (honest) servers, then the path header (S, W) should also be signed (as in the next section). Otherwise, the attacker might redirect an envelope from one web service to another.

3.4 X.509 Signature

The next protocol does not depend on password-based authentication. Instead, it uses public-key signatures based on X.509 certificates. We assume that the user u has a public/private key pair and keeps the private key secret. We also assume that u and S agree on the public key k_r of some X.509 certification authority, and that this authority issued only one certificate for u, with u's public key.

In contrast with password-based signatures, X.509 signature tokens cannot use fragments of the username token as message identifier. Instead, they can sign the globally unique identifier included in the path header of our SOAP messages, as defined in WS-Routing [33]. This is reflected by the following additional predicates:

- $\mathit{isX509Token}(tok, k_r, u, a, k)$ means that tok is a binary token that contains a certificate $\mathsf{x509}(s_r, u, a, k)$ with certifier's public key $k_r = \mathsf{pk}(s_r)$.
- $\mathit{isSigVal}(sv, si, k, a)$ is extended with a clause that checks signatures using the $\mathsf{rsa\text{-}sha1}$ algorithm.
- $\mathit{hasPathHeader}(e, ac, to, id, ea, et, ei)$ means that envelope e has a path header

with action ac, destination to, and message identifier id in elements ea, et, and ei, respectively.

- $\mathit{hasX509SignedBody}(e, k_r, u, ac, to, id, b, ea, et, ei)$ is the top-level predicate. It means that the envelope e has an X.509 token for u certified by k_r whose public key signs the body b and a path header ea, et, ei containing ac, to, id.

```
isX509Token(tok : item, k_r : bytes, u : string, a : string, k : bytes) :-
  tok = <BinarySecurityToken _>base64(xcert)</>,
  check-x509(xcert, k_r) = k_r,
  u = x509-user(xcert),
  a = x509-alg(xcert),
  k = x509-key(xcert).

isSigVal(sv : bytes, si : item, k : bytes, a : string) :-
  a = rsa-sha1, check-rsa-sha1(c14n(si), sv, k) = k.

hasPathHeader(e : item, ac, to, id : string, ea, et, ei : item) :-
  e = <Envelope><Header>headers</>_</>,
  header ∈ headers,
  header = <path _>ea et ei</>,
  ea = <action _>ac</>,
  et = <to _>to</>,
  ei = <id _>id</>.

hasX509SignedBody(e : item, k_r : bytes, u, ac, to, id : string,
                                               b, ea, et, ei : item) :-
  hasBody(e, b),
  hasPathHeader(e, ac, to, id, ea, et, ei),
  hasSecurityHeader(e, toks),
  xtok ∈ toks,
  isX509Token(xtok, k_r, u, rsa-sha1, k),
  sig ∈ toks,
  isSignature(sig, rsa-sha1, k, b, ea, et, ei).
```

The message exchange for the X.509 signature protocol is almost the same as the one in Section 3.3, with two differences. First, the contents of the log entries is now $u\ W\ S\ id\ \mathit{OrderId}$ (instead of $u\ n\ t\ \mathit{OrderId}$). Second, we use the top-level predicate $\mathit{hasX509SignedBody}(e, k_r, u, W, S, id, b, ea, et, ei)$ instead of $\mathit{hasUserSignedBody}(e, u, pwd, n, t, b)$. The predicate checks $ac = W$ and $to = S$ in the path header by unification.

Event 1:	I logs `<Begin>`$u\ W\ S\ id\ \mathit{OrderId}$`</>`
Message 1:	$I \to S, W \quad e$ where $\mathit{hasX509SignedBody}(e, k_r, u, W, S, id, b, ea, et, ei)$, and $\mathit{isGetOrder}(b, \mathit{OrderId})$

Event 2: S logs `<End>`$u\ W\ S\ id\ \mathit{OrderId}$`</>`
Message 2: $S \rightarrow I \quad e'$
where $\mathit{hasBody}(e', b')$,
and $\mathit{isGetOrderResponse}(b', \mathit{OrderId}, u)$

We now obtain the authentication property:

Claim 3 *In the presence of an active Dolev-Yao attacker, if* `<End>`$u\ W\ S\ id\ \mathit{OrderId}$`</>` *is logged by* S*, then* `<Begin>`$u\ W\ S\ id\ \mathit{OrderId}$`</>` *has been logged by* I*.*

This claim can be read as "if S accepts a request from u, then u, at some point, sent this request to S." So by signing the path header, we obtain an additional authenticity guarantee as regards u's intended target (S, W), and thus prevent some redirection attacks. One can easily implement replay protection using the authenticated message identifier. This supposes that clients do generate globally unique identifiers (although this is not actually required to obtain our correspondence property). Alternatively, one may use a custom unique identifier in the envelope body.

3.5 Firewall-Based Authentication

By specifying the structure of security tokens, rather than their use, WS-Security encourages a flexible approach to web service security. For instance, a server may naturally accept both password-based and X.509-based signatures for authentication, leaving that choice to the client. This flexibility yields useful compositional properties in our formal developments. For instance, a web service that runs both protocols is formally equivalent to two web services in parallel, one for each authentication mechanism.

In this section, we illustrate this flexibility with a different composite architecture that chains WS-Security authentication schemes along a WS-Routing path. In addition to a server S and a client I acting on behalf of u, we consider an intermediate SOAP-level firewall F. The firewall holds the password database, has the X.509 certificate and the corresponding private key for certificate user f, and is responsible for authenticating access to S (and possibly other servers). The client I sends a *GetOrder* request with a password-based signature (for u) to S via F. The path header indicates to F that the message is intended for S. The firewall F checks the password-based signature, adds a new `firewall` header indicating that it has authenticated u, signs the message using f's X.509 certificate, and forwards the message to S. The server S expects an X.509 signature from a particular firewall with certificate user name f. S checks the X.509 signature and certificate, and thus it authenticates the original sender u without knowledge of u's password.

Next, we define (predicates on) the message forwarded by the firewall. To indicate to the server that it has checked the credentials of the user, the firewall adds a new firewall header containing the username token, but with the password digest deleted. It then embeds an X.509 signature that includes this header as well. The predicates for this message are:

- *isFirewallHeader*(h, u, n, t) means that the element h is a firewall header with the username token u, n, t.
- *hasFWHeader*(e, h, u, n, t) means that the envelope e has a firewall header h with u, n, t.
- *hasX509SignedBodyFw*(e, k_r, f, u, n, t, b) is the top-level predicate checked by the server. It means that the envelope e has a firewall header with u, n, t, a body b, and that the firewall header and the body are signed with a valid certificate for f issued by k_r.

```
isFirewallHeader(h : item, u : string, n : bytes, t : string) :-
  h = <firewall _>utok</>,
  utok = <UsernameToken>
           <Username>u</>
           <Nonce>base64(n)</>
           <Created>t</>.

hasFWHeader(e, h : item, u : string, n : bytes, t : string) :-
  e = <Envelope ><Header>headers</>_</>,
  h ∈ headers,
  isFirewallheader(h, u, n, t).

hasX509SignedBodyFw(e : item, k_r : bytes, f, u : string,
                                  n : bytes, t : string, b : item) :-
  hasBody(e, b),
  hasFWHeader(e, h, u, n, t),
  hasSecurityHeader(e, toks),
  xtok ∈ toks,
  isX509Token(xtok, k_r, f, rsa-sha1, p),
  sig ∈ toks,
  isSignature(sig, rsa-sha1, p, b, h).
```

The protocol involves three messages, as follows:

```
   Event 1:  I logs <Begin>u n t OrderId</>
 Message 1:  I → F, W    e
             where hasUserSignedBody(e, u, pwd, n, t, b)
 Message 2:  F → S, W    e'
             where hasX509SignedBodyFw(e', k_r, f, u, n, t, b)
             and isGetOrder(b, OrderId)
   Event 2:  S logs <End>u n t OrderId</>
 Message 3:  S → I    e''
             where hasBody(e'', b')
             and isGetOrderResponse(b', OrderId, u)
```

In terms of the SOAP specification, the two envelopes e and e' represent two stages in the lifetime of the same message: it is sent by the client endpoint, updated by the firewall intermediary, and received by the server endpoint.

Claim 4 *In the presence of an active Dolev-Yao attacker, if* `<End>`$u\ n\ t$ *OrderId*`</>` *is logged by S, then* `<Begin>`$u\ n\ t$ *OrderId*`</>` *has been logged by I.*

Thus, we obtain the same end-to-end authenticity guarantee as with the password-based signature protocol of Section 3.3, but for a different implementation that does not require S to know u's password. We prove this claim by composing the correspondence property for the password-based signature in Message 1 with that for the X.509 signature in Message 2.

4 A Pi Calculus Semantics

In order to formalize and validate the claims of Section 3, we specify the behaviour of the participants (and in particular their implementation of predicates) as processes in the applied pi calculus. We refer to Appendix A for a brief overview of the calculus and its main notations, and to [1] for its semantics. Here, we use the sorts, terms, and equations described in Section 2, with coercion functions from strings to items, and with additional sorts for communication channels [30]. (However, in our model, channels do not appear in terms of other sorts, nor in messages sent on channels.) We always assume that terms, formulas, processes, and contexts are well-sorted, but usually keep sort information implicit.

This section divides into the following parts. Section 4.1 describes our computational interpretation of formulas as certain nondeterministic processes in the applied pi calculus. Section 4.2 introduces formal notions of robust safety—that embedded correspondence assertions hold in spite of the presence of an attacker—and functional adequacy—that a protocol may run to successful completion in the absence of an attacker. Section 4.3 uses these definitions to state results about the password-based signature protocol of Section 3.3. Theorem 1 asserts that a process formalizing this protocol is robustly safe—Claim 2 is a corollary. Moreover, Theorem 2 asserts the formalization is functionally adequate. Section 4.4 breaks the proof of Theorem 1 into two halves: first, the definition and proof of correctness of a simpler, core protocol; second, the proof that the correctness of the core protocol implies Theorem 1. Section 4.5 describes how to generalize our results to configurations with multiple servers and users. Sections 4.6 and 4.7 state and prove similar robust safety properties for the protocols of Sections 3.4 (with X.509 signatures) and 3.5 (with an intermediate firewall), respectively; we obtain Claims 3 and 4 as corollaries. We do not include a proof of Claim 1, concerning the weak protocol of Section 3.2 that uses password-digests. We conjecture that a proof could be obtained by adapting and simplifying the proof of Theorem 1, concerning the stronger protocol that uses password-based signatures (and still supports password-digests).

4.1 Interpretation of Formulas

We describe a (partial) implementation of our logic in the applied pi calculus. We inductively define processes of the form *filter* $\Phi \mapsto \widetilde{y}$ *in* P, where the variables $\widetilde{y}$ are bound in P and get assigned to terms making the formula Φ true. When the formula is an equality $V = T$ we assume that one of the terms is known, and that the other can be treated as a pattern, matching variables to known subterms in the known term. In the following formal definitions, we always assume that V is the known term, and that T is the pattern, but in our example predicates we allow either of the terms to be the pattern. For a pattern to be implementable, there must be an inverse term for each bound variable, able to compute the value of the variable from the known term.

Patterns:

The equality $V = T$ binds variables $\widetilde{y}$ with pattern T, written $V = T \mapsto \widetilde{y}$, when (1) $\widetilde{y} \subseteq fv(T) \setminus fv(V)$, and (2) T has *inverse terms* $\widetilde{S}$, with $fv(\widetilde{S}) \subseteq \{x\}$, $fn(\widetilde{S}) = \varnothing$, and, for all terms $U, \widetilde{W}$, if $U = T\{\widetilde{y} = \widetilde{W}\}$, then $\widetilde{W} = \widetilde{S}\{x = U\}$.

For instance, the pattern $\mathsf{base64}(y)$ has inverse $S \triangleq \mathsf{i\text{-}base64}(x)$; for all V and W, if $V = \mathsf{base64}(W)$ then $W = S\{x = V\} = \mathsf{i\text{-}base64}(\mathsf{base64}(W))$. On the other hand, the pattern $\mathsf{sha1}(y)$ has no inverse, and therefore would not satisfy point (2).

The following table is the partial inductive definition of *filter* $\Phi \mapsto \widetilde{y}$ *in* P. If such a process is defined by the following rules, we say that the formula Φ is *implementable* with bound variables $\widetilde{y}$. When *filter* $\Phi \mapsto \widetilde{y}$ *in* P is defined and closed, we intend that it seeks closed terms $\widetilde{V}$ such that $\models \Phi\{\widetilde{y} = \widetilde{V}\}$, and acts as $P\{\widetilde{y} = \widetilde{V}\}$. Lemma 1 makes this precise.

Formula Implementation: *filter* $\Phi \mapsto \widetilde{y}$ *in* P **when** $\widetilde{y} \subseteq fv(\Phi)$

filter $V = T \mapsto \widetilde{y}$ *in* $P \quad \triangleq$

$\quad$ *let* $\widetilde{y} = \widetilde{S}\{x = V\}$ *in if* $V = T$ *then* P

$\quad$ when $V = T \mapsto \widetilde{y}$ with inverse terms $\widetilde{S}$

filter $x \in V \mapsto x$ *in* $P \quad \triangleq$

$\quad \nu s, c.(c(x).P \mid \overline{s}\langle V\rangle \mid !s(z).\mathit{filter}\ z = h\ t \mapsto h, t\ \mathit{in}\ (\overline{c}\langle h\rangle \mid \overline{s}\langle t\rangle))$

$\quad$ when $x \notin fv(V)$ and with $\{s, c\} \cap fn(P) = \varnothing$

filter $p(\widetilde{V}) \mapsto \widetilde{y}$ *in* $P \quad \triangleq$

$\quad \nu s.(\overline{s}\langle \epsilon\rangle \mid \prod_{i \in 1..m} s(\_).\mathit{filter}\ \Phi_i\{\widetilde{x} = \widetilde{V}\} \mapsto \widetilde{y}, \widetilde{z}_i\ \mathit{in}\ P)$

$\quad$ when $p(\widetilde{x})$:- $\Phi_1 \vee \cdots \vee \Phi_m$, $s \notin fn(P)$

$\quad$ and, $\forall i \in 1..m, fv(\Phi_i) = \widetilde{x} \uplus \widetilde{z}_i$ and $(fv(\widetilde{V}) \cup fv(P)) \cap \widetilde{z}_i = \varnothing$

filter $\Phi_1, \Phi_2 \mapsto \widetilde{y}$ *in* $P \quad \triangleq$

$\quad$ *filter* $\Phi_1 \mapsto (\widetilde{y} \cap fv(\Phi_1))$ *in* (*filter* $\Phi_2 \mapsto (\widetilde{y} \setminus fv(\Phi_1))$ *in* P)

When $V = T \mapsto \widetilde{y}$, with inverse terms $\widetilde{S}$, the implementation *filter* $V = T \mapsto \widetilde{y}$ *in* P binds the variables $\widetilde{y}$ of the pattern T to components of the term V, and verifies that hence the pattern matches the term. If so, the match succeeds, and P runs. Otherwise, the match fails, and the implementation deadlocks.

When $x \notin \mathit{fv}(V)$, the implementation $\mathit{filter}\ x \in V \mapsto x\ \mathit{in}\ P$ outputs V on a fresh channel s, and runs the process $!s(z).\mathit{filter}\ z = h\ t \mapsto h, t\ \mathit{in}\ (\overline{c}\langle h\rangle \mid \overline{s}\langle t\rangle)$ which binds $h = V_1$ and $t = V_2\ \ldots\ V_m\ \epsilon$, provided $V = V_1\ V_2\ \ldots\ V_m\ \epsilon$ with $m \geq 1$, then outputs h on c, and t on the fresh channel s. The effect of this replication is to output each of the terms $V_1, \ldots, V_m$ on the fresh channel c. The process $c(x).P$ is the only listener on c; so the outcome is $P\{x = V_i\}$ for one $i \in 1..m$. If, in fact, V is the empty list, the implementation deadlocks.

When $p(\widetilde{x})$ `:-` $\Phi_1 \vee \cdots \vee \Phi_m$, the implementation $\mathit{filter}\ p(\widetilde{V}) \mapsto \widetilde{y}\ \mathit{in}\ P$ generates a separate process $s(\_).\mathit{filter}\ \Phi_i\{\widetilde{x} = \widetilde{V}\} \mapsto \widetilde{y}, \widetilde{z}_i\ \mathit{in}\ P$ for each clause $i \in 1..m$, where $\widetilde{z}_i$ are the local variables for clause i. We make an internal choice of which to run by arranging all to listen on the fresh channel s, on which only a single message is sent. We are assuming that $\widetilde{y} \subseteq \mathit{fv}(\widetilde{V})$, which with the side-condition $\mathit{fv}(\Phi_i) = \widetilde{x} \uplus \widetilde{z}_i$, yields that $\mathit{fv}(\Phi_i\{\widetilde{x} = \widetilde{V}\}) = \mathit{fv}(\widetilde{V}) \uplus \widetilde{z}_i$ for each i. Therefore, the formula implementation $\mathit{filter}\ \Phi_i\{\widetilde{x} = \widetilde{V}\} \mapsto \widetilde{y}, \widetilde{z}_i\ \mathit{in}\ P$ satisfies the well-formedness condition $\widetilde{y}, \widetilde{z}_i \subseteq \mathit{fv}(\Phi_i\{\widetilde{x} = \widetilde{V}\})$. Moreover, the side-condition $\mathit{fv}(P) \cap \widetilde{z}_i = \varnothing$ guarantees there is no confusion between the local variables $\widetilde{z}_i$ and any variables in P.

The implementation $\mathit{filter}\ \Phi_1, \Phi_2 \mapsto \widetilde{y}\ \mathit{in}\ P$ works by evaluating Φ_1 then Φ_2 before running P.

As an example, we show an implementation of $\mathit{hasBody}(e, b)$:

$$
\begin{array}{rl}
\multicolumn{2}{l}{\mathit{filter}\ \mathit{hasBody}(e,b) \mapsto b\ \mathit{in}\ [\text{-}]} \\
= & \nu s.(\overline{s}\langle\epsilon\rangle \mid s(\_). \\
& \quad \mathit{filter}\ e = \texttt{<Envelope><Header>}y_1\texttt{</>}b\texttt{</>} \mapsto y_1, b\ \mathit{in} \\
& \qquad \mathit{filter}\ b = \texttt{<Body }y_2\texttt{>}y_3\texttt{</>} \mapsto y_2, y_3\ \mathit{in}\ [\text{-}]) \\
= & \nu s.(\overline{s}\langle\epsilon\rangle \mid s(\_). \\
& \quad \mathit{let}\ y_1 : \mathsf{items} = \texttt{Header}.\mathsf{body}(\mathsf{hd}(\texttt{Envelope}.\mathsf{body}(e)))\ \mathit{in} \\
& \quad \mathit{let}\ b : \mathsf{item} = \mathsf{hd}(\mathsf{tl}(\texttt{Envelope}.\mathsf{body}(e)))\ \mathit{in} \\
& \quad \mathit{if}\ e = \texttt{<Envelope><Header>}y_1\texttt{</>}\ b\ \epsilon\texttt{</>}\ \mathit{then} \\
& \qquad \mathit{let}\ y_2 : \mathsf{atts} = \texttt{Body}.\mathsf{att}(b)\ \mathit{in} \\
& \qquad \mathit{let}\ y_3 : \mathsf{items} = \texttt{Body}.\mathsf{body}(b)\ \mathit{in} \\
& \qquad \mathit{if}\ b = \texttt{<Body }y_2\texttt{>}y_3\texttt{</>}\ \mathit{then}\ [\text{-}])
\end{array}
$$

To state the correctness of the embedding of our logic within the applied pi calculus, we appeal to the following notion of *internal choice*. We write $\rightarrow^*$ for a series of reduction steps and $\sim$ for strong bisimilarity, the strong form of observational equivalence [1]. For any set of processes X, we co-inductively define the set of processes $\bigoplus X$ that are internal choices of X:

Internal Choice: $\bigoplus X$.

A process Q is an internal choice on X, written $Q \in \bigoplus X$, if and only if (1) if $P \in X$ then $Q \rightarrow^* \sim P$; (2) if $Q \rightarrow Q'$, then either $Q' \sim P$ with $P \in X$ or $Q' \in \bigoplus Y$ with $Y \subseteq X$; and (3) Q does not communicate on free channel names.

Lemma 1 *If filter $\Phi \mapsto \widetilde{y}$ in P is defined and closed then:*

$$\mathit{filter}\ \Phi \mapsto \widetilde{y}\ \mathit{in}\ P \quad \in \quad \bigoplus\{P\{\widetilde{y} = \widetilde{V}\} \mid \mathit{fv}(\widetilde{V}) = \varnothing \wedge \models \Phi\{\widetilde{y} = \widetilde{V}\}\}$$

The proof appears in Appendix B.

4.2 Safety Properties, Functional Properties

To formalize the authenticity properties claimed in Section 3, we mark the progress of the client and server processes with begin- and end-events, represented as message outputs on the channels *begin* and *end*, respectively. Hence, our authenticity properties become non-injective correspondence assertions [41] between messages. We write $\approx$ for (weak) observational congruence in applied pi. Further, to capture the occurrence of events, we define a derived notion of observation of messages on free channels:

Event Occurrence: $A \triangleright \overline{a}\langle V\rangle$

A outputs the term V on channel a, written $A \triangleright \overline{a}\langle V\rangle$, when $A \approx \overline{a}\langle V\rangle \mid A'$.

Much as in Gordon and Jeffrey's formulation of correspondence assertions [21], we define safety and robust safety: a process is safe if every end-event has a matching begin-event, and is robustly safe if it is safe in the presence of any opponent.

Safety and Robust Safety:

A is *safe* if and only if, whenever $A \rightarrow^* B$, $B \triangleright \overline{\mathit{end}}\langle V\rangle$ implies $B \triangleright \overline{\mathit{begin}}\langle V\rangle$.
A is *robustly safe* if and only if, for all evaluation contexts E[-] where the channels *begin* and *end* do not occur, $E[A]$ is safe.

Intuitively, E[-] represents any active attacker (in the applied pi calculus) that controls both the network and the client application behaviour, A is the initial configuration of the protocol being considered, and B represents any reachable state of the protocol, after interleaving any number of sessions.

In addition to security properties such as robust safety, one should check that the protocol works as intended and may indeed succeed, at least in the absence of an attacker. The following definition captures this intent for a process A that begins the protocol for V:

Functional Adequacy:

A is *functionally adequate for* V when $A \rightarrow^* B$ with $B \triangleright \overline{\mathit{end}}\langle V\rangle$ for some B.

The next lemma states that our main security properties can be established using the theory of observational equivalence in the applied pi calculus.

Lemma 2 *Suppose $A \approx B$. If A is robustly safe then so is B. Moreover, if A is functionally adequate for V then so is B.*

Proof For robust safety, assume $E[B] \rightarrow^* B' \triangleright \overline{end}\langle V\rangle$ for some evaluation context $E[\text{-}]$ that does not contain *begin* or *end*. We have $E[A] \approx E[B]$ (by context-closure of $\approx$), $E[A] \rightarrow^* A'$ with $A' \approx B'$ (by weak simulation), $A' \triangleright \overline{end}\langle V\rangle$ (since $\approx$ preserves $\triangleright \overline{end}\langle V\rangle$), $A' \triangleright \overline{begin}\langle V\rangle$ (by robust safety of A), and thus $B' \triangleright \overline{begin}\langle V\rangle$ (since $\approx$ preserves $\triangleright \overline{begin}\langle V\rangle$).

For functional adequacy, assume $A \rightarrow^* A' \triangleright \overline{end}\langle V\rangle$. From $A \approx B$ we get $B \rightarrow^* B'$ with $A' \approx B'$ and thus $B' \triangleright \overline{end}\langle V\rangle$. □

Moreover, logical equivalence, when lifted to processes, also preserves robust safety.

Logical Equivalence of Processes:

Two processes are logically equivalent when they differ only in their choices of implementable, logically-equivalent formulas.

Lemma 3 *Logical equivalence preserves robust safety.*

The proof appears in Appendix B.3.

4.3 Stating Password-Based Authentication

We are now ready to formulate and prove Claim 2 of Section 3.3 for envelopes with password-based signatures, with or without a password digest. For the sake of simplicity, we focus on protocol configurations $\mathcal{Q}$ with a single user u, with initiator process I_u and a single server S_u that share a secret password with that user, represented as a restricted name s_{pwd}. The two parts of the protocol also share a communication channel, *http*. Since *http* is not restricted, an environment that encloses $\mathcal{Q}$ can also read, modify, and write any SOAP message.

Protocol Configurations: $\mathcal{Q}$ (parameterized by *Envelope*)

$$\begin{array}{rcl}
\mathcal{Q} & \triangleq & \nu s_{pwd}.(\{u = \mathsf{principal}(s_{pwd})\} \mid I_u \mid S_u) \\
I_u & \triangleq & !init_u(n,t,b).(\overline{begin}\langle u\ n\ t\ b\rangle \mid \overline{http}\langle Envelope\rangle) \\
S_u & \triangleq & !http(e).filter\ hasUserSignedBody(e,u',s_{pwd},n,t,b) \\
& & \qquad \mapsto u',n,t,b\ in\ \overline{end}\langle u'\ n\ t\ b\rangle
\end{array}$$

The initiator, I_u, repeatedly receives high-level requests on a control channel $init_u$. Using that control channel, the environment can thus initiate any number of requests on behalf of u, for any terms N, TS, B. These requests are deemed genuine: they are echoed on channel *begin*. The process I_u is also parameterized by a term *Envelope* that determines the actual SOAP envelopes constructed and sent by the initiator.

The server, S_u, repeatedly receives low-level envelopes on channel *http*, filters them using the top-level predicate defined in Section 3.3 (one easily checks that this predicate is implementable) and finally sends a message on channel *end* for each accepted envelope. (More generally, we would represent a server that accepts requests from users $u_1, \ldots, u_m$ as a parallel composition $\prod_{i \in 1..m} S_{u_i}$.)

The scope restriction on s_{pwd} models our secrecy assumption on the password, essentially supposing that it is a strong secret shared between the initiator and the server and used only in this kind of envelope.

The active substitution $\{u = \mathsf{principal}(s_{pwd})\}$ binds the variable u to the expression $\mathsf{principal}(s_{pwd})$, and exports u (but not s_{pwd}) to the environment.

Crucially, we do not want our robust safety result to depend on every detail of the envelope. Instead, we express minimal requirements as follows:

Safe Envelopes:

A *safe envelope* is a term of the form $\mathit{Envelope} = T\varphi$, for any terms T and SI such that $s_{pwd} \notin \mathit{fn}(T, SI)$ and $\mathit{isSigInfo}(SI, \texttt{hmac-sha1}, b)$ is valid, with the active substitution φ defined by:

$$\begin{aligned}\varphi \quad \triangleq \quad & \{d = \mathsf{sha1}(\mathsf{concat}(n, \mathsf{concat}(\mathsf{utf8}(t), \mathsf{utf8}(s_{pwd})))), \\ & \; sv = \mathsf{hmac\text{-}sha1}(\mathsf{p\text{-}sha1}(s_{pwd}, \mathsf{concat}(n, \mathsf{utf8}(t))), \mathsf{c14n}(SI))\}\end{aligned}$$

To elaborate, as regards safety properties, *Envelope* may be any XML term, as long as the password occurs at most in the digest and signature values. Similarly, most of the subterms in the signature information are irrelevant for safety, even if they happen to be signed in SI.

Theorem 1 *For any safe envelope, the configuration $\mathcal{Q}$ is robustly safe.*

From this theorem and the definition of $\mathit{isGetOrder}(b, \mathit{orderId})$, we easily derive the more specific claim of Section 3.3. We devote Section 4.4 to the proof of Theorem 1.

For functional adequacy, the structure of the envelope is more constrained. For example, T and SI can be instantiated as follows:

```
T ≜ <Envelope>
      <Header>
        <Security>
          <UsernameToken Id="utoken">
            <Username>u</>
            <Password Type="PasswordDigest">
              base64(d)
            <Nonce>base64(n)</>
            <Created>t</>
          <Signature>
            SI
            <SignatureValue>base64(sv)</>
            <KeyInfo>
              <SecurityTokenReference>
                <Reference URI="#utoken"></>
      b
```

$SI \triangleq$ `<SignedInfo>`
```
    <CanonicalizationMethod Algorithm="c14n"></>
    <SignatureMethod Algorithm="hmac-sha1"></>
    <Reference URI="#body">
      <Transforms>
        <Transform Algorithm="c14n"></>
      <DigestMethod Algorithm="sha1"></>
      <DigestValue>base64(sha1(c14n(b)))</>
```

Theorem 2 *The envelope $T\varphi$ with T and SI defined above is safe and, for any ground terms N : bytes, TS : string, B : item with $B =$ `<Body Id="body">_</>`, the configuration $\overline{init_u}\langle N, TS, B\rangle \mid \mathcal{Q}$ with that envelope is functionally adequate for the term $u\ N\ TS\ B$.*

Proof We easily check that $T\varphi$ is a safe envelope and that

$$\models hasUserSignedBody(T\varphi, \mathsf{principal}(s_{pwd}), s_{pwd}, N, TS, B)$$

Then we apply Lemma 1. We obtain

$$\overline{init}\langle N, TS, B\rangle \mid \mathcal{Q} \quad \rightarrow\rightarrow (\rightarrow^{*}\sim) \quad \overline{begin}\langle u\ N\ TS\ B\rangle \mid \overline{end}\langle u\ N\ TS\ B\rangle \mid \mathcal{Q}$$

with two communication steps (on $init_u$ and $http$) followed by the reduction steps and equivalence of condition (1) of internal choice (in some evaluation context). □

Conversely, by Theorem 1, if we have both $\overline{init_u}\langle N, TS, B\rangle \mid \mathcal{Q} \rightarrow^{*} A$ and also $A \triangleright \overline{end}\langle u'\ N'\ T'\ B'\rangle$, then $A \triangleright \overline{begin}\langle u'\ N'\ T'\ B'\rangle$ and, since a single message is sent on *begin*, we obtain that $u', N', T', B' = u, N, TS, B$.

4.4 Proving Password-Based Authentication

We now present a proof of Theorem 1. An intuition behind the proof is that the security property relies only on a few elements in the envelope. For instance, the signature bytes are sufficient for authentication, whereas the other elements in the envelope only provide the server with (untrusted) hints to verify the signature. Hence, to establish robust safety, we rely on a stronger, more specific lemma about a core protocol that explicitly deals only with these bytes.

The proof is in two stages. First, we show how the password-based signature protocol can be decomposed into a "core protocol" that deals with authentication and an XML wrapper. The XML wrapper has no access to the password, and need not be trusted: formally, it becomes part of the hostile environment. We show that it is enough to prove robust safety for the core protocol (Lemma 5). In the second stage, we prove that the core protocol itself is robustly safe (Lemma 9) by exhibiting an invariant on its reachable states (Lemma 8).

We decompose

$$hasUserSignedBody(e, u, pwd, n, t, b) \mapsto u, n, t, b$$

into two implementable formulas

$$\begin{aligned}&\mathit{hasUserSignatureEvidence}(e,u,n,t,b,sv,si) \mapsto u,n,t,b,sv,si,\\ &\mathit{checkEvidence}(sv,si,u,pwd,n,t,b) \mapsto \varnothing\end{aligned}$$

hasUserSignatureEvidence parses the envelope and extracts the bits that are needed to verify the signature; it has no access to the password. All the checks related to authentication are contained in *checkEvidence*. These predicates are defined by:

```
checkEvidence(sv : bytes, si : item, u, pwd : string, n : bytes,
                                  t : string, x_1, ..., x_m : item) :-
  isSigInfo(si, hmac-sha1, x_1, ..., x_m),
  u = principal(pwd),
  k = p-sha1(pwd, concat(n, utf8(t))),
  isSigVal(sv, si, k, hmac-sha1).

isUserToken(tok : item, u, n : bytes, t : string) :-
  tok = <UsernameToken _>
          <Username>u</> _
          <Nonce>base64(n)</>
          <Created>t</>.

hasUserSignatureEvidence(e : item, u : string, n : bytes, t : string,
                                  b : item, sv : bytes, si : item) :-
  hasBody(e, b),
  hasSecurityHeader(e, toks),
  utok ∈ toks,
  isUserToken(utok, u, n, t),
  sig ∈ toks,
  sig = <Signature _>si <SignatureValue>base64(sv)</> _</>.
```

We verify the correctness of this decomposition in terms of logical equivalence:

Lemma 4 *The two formulas*

$\mathit{hasUserSignedBody}(e,u,pwd,n,t,b)$ *and*
$\mathit{hasUserSignatureEvidence}(e,u,n,t,b,sv,si), \mathit{checkEvidence}(sv,si,u,pwd,n,t,b)$

are logically equivalent.

Proof The two formulas are equal up to a permutation of conjunctive clauses with disjoint variables. □

Using this decomposition, we define the core protocol configuration $\mathcal{Q}^\circ$, a counterpart of $\mathcal{Q}$ for the simpler predicate *checkEvidence* that binds no variables, and for replicated processes I°_u and S°_u that communicate with the environment on channels c and s, respectively, instead of channel *http*.

Core Protocol Configurations: $\mathcal{Q}^\circ$ (parameterized by SI)

$$\begin{array}{rcl}
\mathcal{Q}^\circ[\text{-}] & \triangleq & \nu s_{pwd}.(\{u = \mathsf{principal}(s_{pwd})\} \mid I_u^\circ \mid S_u^\circ \mid [\text{-}]) \\
I_u^\circ & \triangleq & !init_u(n,t,b).(\overline{begin}\langle u\ n\ t\ b\rangle \mid \overline{c}\langle d, sv, SI, u, n, t, b\rangle\varphi) \\
S_u^\circ & \triangleq & !s(sv, si, u', n, t, b).filter\ checkEvidence \\
 & & \quad (sv, si, u', s_{pwd}, n, t, b) \mapsto \varnothing\ in\ \overline{end}\langle u'\ n\ t\ b\rangle
\end{array}$$

We write $\mathcal{Q}^\circ$ for $\mathcal{Q}^\circ[\mathbf{0}]$ (the initial state of the core protocol).

Lemma 5 shows that this core protocol is logically equivalent, under an evaluation context, to the original protocol. This implies that if $\mathcal{Q}^\circ$ is robustly safe, so is $\mathcal{Q}$.

Lemma 5 (XML/Core) *For any safe envelope, there exists an evaluation context $E_\mathcal{Q}[\text{-}]$ where the names begin, end do not occur and a process $\mathcal{Q}^\bullet$ logically equivalent to $\mathcal{Q}$ such that $\mathcal{Q}^\bullet \approx E_\mathcal{Q}[\mathcal{Q}^\circ]$.*

Proof For a given safe envelope, $T\varphi$, with SI replaced by si, we let $\mathcal{Q}^\bullet$ be $\mathcal{Q}$ up to the logical equivalence of Lemma 4 and let $E_\mathcal{Q}[\text{-}]$ be the evaluation context

$$E_\mathcal{Q}[\text{-}] \quad \triangleq \quad \nu c, s. \left(\begin{array}{l}
[\text{-}] \mid \\
!c(d, sv, si, u, n, t, b).\overline{http}\langle T\varphi\rangle \mid \\
!http(e).\ filter\ hasUserSignatureEvidence(e, u', n, t, b, sv, si) \\
\qquad\qquad \mapsto u', n, t, b, sv, si\ in\ \overline{s}\langle sv, si, u', n, t, b\rangle
\end{array} \right)$$

for some $c, s \notin fn(T)$. $E_\mathcal{Q}[\mathcal{Q}^\circ]$ differs from $\mathcal{Q}^\bullet$ in two ways:

(1) Instead of I_u, there is an extra communication on channel c after computing d and si, but before sending messages on *begin* and *http*.

(2) Instead of S_u, there is an extra communication on channel s after checking *hasUserSignatureEvidence* but before checking predicate *checkEvidence*.

Since c and s are both restricted channels used only either for asynchronous outputs or as a single replicated input, these extra communication steps do not affect $\approx$.□

To prove robust safety for the core protocol, we first define the valid states of the core protocol in an evaluation context. Valid states are our correctness invariant. They describe protocol states reachable from $\mathcal{Q}^\circ$ after unfolding n sessions, in which no secrets have been leaked and only messages sent by the client have been accepted by the server.

Valid States for the Core Protocol:

(1) φ_i is adapted from φ in the definition of safe envelopes with variables d_i, sv_i, n_i, t_i, b_i and term SI_i instead of d, sv, n, t, b and SI.
(2) A *session state* is a process of the form $C_i = \overline{begin}\langle u\ n_i\ t_i\ b_i\rangle \mid \varphi_i \mid J_i$ where J_i is any parallel composition of processes from $\{\overline{end}\langle u\ n_i\ t_i\ b_i\rangle\} \cup \bigoplus\{\overline{end}\langle u\ n_i\ t_i\ b_i\rangle\} \cup \bigoplus\{\}$. ($C_i$ has free variables u, n_i, t_i, b_i and defined variables d_i, sv_i.)

(3) An *internal state* is a parallel composition of session states $C = \prod_{i<m} C_i$, for some $m \geq 0$.
(4) A *valid state* is a closed process of the form $A = E[\mathcal{Q}^\circ[C]]$ where $E[\text{-}]$ is an evaluation context where *begin* and *end* do not occur and C is an internal state.

For a given internal state C, let σ_C be the (ordinary) substitution obtained by composing $\{u = \mathsf{principal}(s_{pwd})\}$ and each φ_i for $i < m$. By definition, the frame obtained from $\mathcal{Q}^\circ[C]$, which represents the attacker's knowledge about s_{pwd}, is $\varphi_C = \nu s_{pwd}.\sigma_C$. We consider the effect of σ_C on the predicate *checkEvidence* in Lemma 7, to follow. First, we develop some basic properties of our equational theory on terms.

Our equational theory is defined as the term-rewriting system obtained from the (oriented) rewrite rules of Section 2. We give some basic definitions and results for this system.

Redex, Normal Form, Selector:

A term T is a *redex* for the (oriented) rewrite rule $V = W$ when T is $V\sigma$ for some substitution σ. Then, $W\sigma$ is the result of the rewriting.
A term T is in *normal form* when it contains no redex for any rule; it is a normal form of V when $V = T$.
A function symbol f is a *selector* when there is a rewrite rule of the form $\mathsf{f}(\widetilde{V}) = W$.

Lemma 6

(1) *Every term has a unique normal form.*

(2) *Two terms are equal if and only if their normal forms are identical.*

(3) *Suppose* f *is one of the function symbols* $\mathsf{sha1}$, $\mathsf{hmac\text{-}sha1}$, $\mathsf{p\text{-}sha1}$, *or* $\mathsf{principal}$. *If terms* U *and* $\mathsf{f}(\widetilde{V})$ *are in normal form, and* $\mathsf{f}(\widetilde{V})$ *does not occur as a subterm of* U, *then* $U\{x = \mathsf{f}(\widetilde{V})\}$ *is also in normal form.*

(4) *If* $\mathsf{f}(\widetilde{U}) = \mathsf{g}(\widetilde{V})$, *then either* f *or* g *is a selector, or* $\mathsf{f} = \mathsf{g}$ *and* $\widetilde{U} = \widetilde{V}$.

(5) *If* $\mathsf{f}(\widetilde{U}) = \mathsf{g}(\widetilde{V})$, *where* $\widetilde{U}, \widetilde{V}$ *are normal, then either*

(a) $\mathsf{f} = \mathsf{g}$ *and* $(\widetilde{U} = \widetilde{V})$, *or*

(b) $\mathsf{f}(\widetilde{V})$ *is a redex, or*

(c) $\mathsf{g}(\widetilde{W})$ *is a redex.*

Proof Let $U \mapsto V$ be the reduction relation obtained by orienting our equations on terms from left to right, and closing under contexts. By standard rewriting techniques [4], our equational theory is the reflexive, transitive, symmetric closure of $U \mapsto V$. Whenever $U \mapsto V$ then V has fewer function symbols than U, so $\mapsto$ is terminating. Our term rewriting system has no critical pairs; each selector symbol appears only as the outermost symbol in a rule, and no two rules directly overlap.

Given that the reduction relation is terminating and has no critical pairs, it follows that it is confluent. Since $\mapsto$ is terminating and confluent, it follows that (1) every term has a unique normal form, and (2) two terms are equal if and only if their normal forms are identical.

For (3), suppose $\mathsf{f}(\widetilde{V})$ is not a subterm of U, that both are normal, and that $\mathsf{f} \in \{\mathsf{sha1}, \mathsf{hmac\text{-}sha1}, \mathsf{p\text{-}sha1}, \mathsf{principal}\}$. Then substituting the term $\mathsf{f}(\widetilde{V})$ for x in U cannot create any redexes, since f does not occur in any rewrite rule, and moreover, since $\mathsf{f}(\widetilde{V})$ does not already occur in U, we cannot complete a redex for either of the selectors $\mathsf{check\text{-}x509}$ and $\mathsf{check\text{-}rsa\text{-}sha1}$ guarded by an implicit term equality. Hence, $U\{x = \mathsf{f}(\widetilde{V})\}$ is in normal form.

For (4), suppose $\mathsf{f}(\widetilde{U}) = \mathsf{g}(\widetilde{V})$ and that neither f nor g is a selector. The normal forms of $\mathsf{f}(\widetilde{U})$ and $\mathsf{g}(\widetilde{V})$ must take the form $\mathsf{f}(\widetilde{U}')$ and $\mathsf{g}(\widetilde{V}')$, since neither f nor g is a selector. These two normal forms must be identical, so it follows that $\mathsf{f} = \mathsf{g}$ and $\widetilde{U}' = \widetilde{V}'$, and hence that $\widetilde{U} = \widetilde{V}$.

For (5), suppose $\mathsf{f}(\widetilde{U}) = \mathsf{g}(\widetilde{V})$ where $\widetilde{U}$ and $\widetilde{V}$ are normal. If either $\mathsf{f}(\widetilde{U})$ or $\mathsf{g}(\widetilde{V})$ is a redex we are done. If neither is a redex, they are two equal normal forms and therefore $\mathsf{f} = \mathsf{g}$ and $(\widetilde{V} = \widetilde{W})$. $\square$

The next lemma states that if a message is received in a valid state of the protocol, and it satisfies the predicate *checkEvidence*, then it must have been sent by the client.

Lemma 7 (*checkEvidence* is safe) *Let C be an internal state with $m \geq 0$ sessions. Let σ' be a substitution that ranges over open terms where the name s_{pwd} does not appear such that $\sigma \triangleq \sigma' \mid \sigma_C$ is closed. If*

$$\models \mathit{checkEvidence}(sv, si, u', s_{pwd}, n, t, b)\sigma$$

then there exists $i < n$ such that $(u', sv, si, n, t, b = u, sv_i, SI_i, n_i, t_i, b_i)\sigma$.

Proof Assume $\models \mathit{checkEvidence}(sv, si, u', s_{pwd}, n, t, b)\sigma$, and let σ_C° be such that $\sigma \equiv \sigma' \mid \sigma_C^\circ$ and σ_C° ranges over closed terms in normal forms. (Hence, $dom(\sigma_C^\circ) = dom(\sigma_C) = \{u\} \cup \{sv_j, d_j | j < m\}$ and, for all $x \in dom(\sigma_C)$, $x\sigma_C^\circ = x\sigma$.)

By definition, $\models \mathit{checkEvidence}(sv, si, u', s_{pwd}, n, t, b)\sigma$ implies there exists σ'' with $dom(\sigma'') = \{k, c, r_1, \mathit{uri}, \mathit{talg}, \mathit{dalg}, \mathit{rest}\}$ such that:

$$\models (u' = \mathsf{principal}(s_{pwd}))\sigma\sigma'' \qquad (1)$$

$$\models (k = \mathsf{p\text{-}sha1}(s_{pwd}, \mathsf{concat}(n, \mathsf{utf8}(t))))\sigma\sigma'' \qquad (2)$$

$$\models (sv = \mathsf{hmac\text{-}sha1}(k, \mathsf{c14n}(si)))\sigma\sigma'' \qquad (3)$$

$$\models (si = \texttt{<SignedInfo>} \; c \; \texttt{<SignatureMethod Algorithm="hmac-sha1"></>} \; r_1 \; \mathit{rest})\sigma\sigma'' \qquad (4)$$

$$\models (r_1 = \texttt{<Reference } \mathit{uri}\texttt{>} \; \mathit{talg} \; \mathit{dalg} \; \texttt{<DigestValue>}\mathsf{base64}(\mathsf{sha1}(\mathsf{c14n}(b)))\texttt{</>})\sigma\sigma'' \qquad (5)$$

In (1), we use the definition of σ_C to introduce u and obtain $(u' = u)\sigma$.
Using (2) to eliminate k in (3), we obtain

$$sv\,\sigma \quad = \quad \mathsf{hmac\text{-}sha1}(\mathsf{p\text{-}sha1}(s_{pwd}, \mathsf{concat}(n\,\sigma, \mathsf{utf8}(t\,\sigma))), \mathsf{c14n}(si\,\sigma)) \qquad (6)$$

Let $T = sv\,\sigma'$ in normal form. We have $sv\,\sigma = T\sigma^\circ_C$ and, by Lemma 6(3) and definition of σ°_C, $T\sigma^\circ_C$ is also in normal form. By plain structural matching on normal forms, we obtain four cases for T:

- $T = x$ for some $x \in dom(\sigma^\circ_C)$ such that $x\sigma^\circ_C = \mathsf{hmac\text{-}sha1}(\_, \_)$, where $\_$ stands for any subterm. By definition of σ°_C, this implies $x = sv_i$ for some $i < k$, and thus $(sv = sv_i)\sigma$.
- $T = \mathsf{hmac\text{-}sha1}(x, \_)$ for some $x \in dom(\sigma^\circ_C)$ such that $x\sigma^\circ_C = \mathsf{p\text{-}sha1}(\_, \_)$.
This is excluded by definition of σ°_C.
- $T = \mathsf{hmac\text{-}sha1}(\mathsf{p\text{-}sha1}(x, \_), \_)$ for some $x \in dom(\sigma^\circ_C)$ such that $x\sigma^\circ_C = s_{pwd}$.
This is excluded by definition of σ°_C.
- $T = \mathsf{hmac\text{-}sha1}(\mathsf{p\text{-}sha1}(s_{pwd}, \_), \_)$.
This is excluded by hypothesis on σ': since $T = sv\,\sigma'$, we have $s_{pwd} \notin fn(T)$.

Using the definition of sv_i in σ_C, equation (6) becomes

$$\begin{aligned} &\mathsf{hmac\text{-}sha1}(\mathsf{p\text{-}sha1}(s_{pwd}, \mathsf{concat}(n_i, \mathsf{utf8}(t_i))), \mathsf{c14n}(SI_i\,\sigma)) \\ = \quad &\mathsf{hmac\text{-}sha1}(\mathsf{p\text{-}sha1}(s_{pwd}, \mathsf{concat}(n\sigma, \mathsf{utf8}(t\sigma))), \mathsf{c14n}(si\,\sigma)) \end{aligned}$$

and thus Lemma 6(4) yields $(si, n, t = SI_i, n_i, t_i)\sigma$. Similarly, using equations (4) and (5) to eliminate si then r_1 in $(si = SI_i)\sigma$, we obtain an equation of the form:

$$(V\{\widetilde{x} = b, uri, talg, dalg, rest\} = V\{\widetilde{x} = b_i, uri_i, talg_i, dalg_i, rest_i\})\sigma$$

for a term V built only from constructors, we obtain $(b = b_i)\sigma$ via Lemma 6(4). $\Box$

Using this lemma, we can show that all reachable configurations of the core protocol are valid states.

Lemma 8 (Invariant Lemma) *If A is a valid state and $A \to T$ then $T \sim A'$ for some valid state A'.*

Proof Our lemma is stated for a particular definition of $\mathcal{Q}^\circ$; however, its proof relies on the process structure of $\mathcal{Q}^\circ$, and is almost parametric in the definitions of φ, *checkEvidence*, and the message content on $init_u$, c, s, *begin*, *end* (as long as Lemma 7 validates these definitions).

Let $A = E[\mathcal{Q}^\circ[C]]$ be a valid core protocol state, with internal state $C = \prod_{i<k} C_i$. We perform a case analysis on the reduction step $A \to A'$. By definition of reduction in applied pi, this step is either a communication or a term comparison. For communication, we must have $A \equiv E'[\overline{a}\langle\widetilde{x}\rangle.P \mid a(\widetilde{x}).Q]$ and $A' \equiv E'[P \mid Q]$ for some channel name a, variables $\widetilde{x}$, processes P and Q, and evaluation context E'[-]. By definition of A and structural equivalence, this implies one of the following cases:

(1) Both the send and receive occur in $\mathcal{Q}^\circ[C]$: we have $A' \equiv E[F[P \mid Q]]$ with $\mathcal{Q}^\circ[C] \equiv F[\overline{a}\langle\widetilde{x}\rangle.P \mid a(\widetilde{x}).Q]$. By definition of core configurations, the channels used for communications in evaluation context in $\mathcal{Q}^\circ[C]$ are *begin*, *end*—only used for sending—and init_u, s—only used for receiving—plus channel names appearing in internal choices.

By property (3) of internal choices, a is thus a local channel in an internal choice P in some parallel composition J_i within C. For some C' and process P', we have, for some internal state P:

$$C \equiv C' \mid P \qquad P \to P' \qquad A' \equiv E[\mathcal{Q}^\circ[C' \mid P']]$$

By definition of J_i, we have $P \in \bigoplus\{\overline{\mathit{end}}\langle u\ n_i\ t_i\ b_i\rangle\} \cup \bigoplus\{\}$. By property (2) of internal choices, we have either $P' \sim \overline{\mathit{end}}\langle u\ n_i\ t_i\ b_i\rangle$ (and we let $P'' = \overline{\mathit{end}}\langle u\ n_i\ t_i\ b_i\rangle$) or $P' \in \bigoplus\{\overline{\mathit{end}}\langle u\ n_i\ t_i\ b_i\rangle\} \cup \bigoplus\{\}$ (and we let $P'' = P'$). In both subcases, $C' \mid P''$ is also an internal state, and we have $A' \equiv E[\mathcal{Q}^\circ[C' \mid P']] \sim E[\mathcal{Q}^\circ[C' \mid P'']]$, which is a valid state.

(2) $\mathcal{Q}^\circ[C]$ sends a message on a free channel: we have $\mathcal{Q}^\circ[C] \equiv F[\overline{a}\langle\widetilde{x}\rangle.P]$ where a is free in $F[\text{-}]$ and $E[\mathcal{Q}^\circ[C]] = E'[a(\widetilde{x}).P \mid \mathcal{Q}^\circ[C]]$. By definition of core configurations, $a \in \{\mathit{begin}, \mathit{end}\}$, so this case is excluded by hypothesis on $E[\text{-}]$.

(3) $\mathcal{Q}^\circ[C]$ receives a message on channel $a \in \mathit{fn}(\mathcal{Q}^\circ[C])$. Using structural equivalence, we can assume that the message output occurs in parallel with [-] in $E[\text{-}]$, and conveys a tuple of any variables that do not occur in $\mathcal{Q}^\circ[C]$. By definition of core configurations, we have either $a = \mathit{init}_u$ using the replicated input in I_u° (case 3a) or $a = s$ using the replicated input in S_u° (case 3b):

(a) We have a valid state A such that:

$$\begin{array}{rcl} A & \equiv & E'[\overline{\mathit{init}_u}\langle u_k, n_k, t_k, b_k\rangle.P \mid \mathcal{Q}^\circ[C]] \\ Q & = & \overline{\mathit{begin}}\langle u\ n_k\ t_k\ b_k\rangle \mid \overline{c}\langle d_k, sv_k, SI_k, u, n_k, t_k, b_k\rangle\varphi_k \\ A' & \equiv & E'[P \mid \mathcal{Q}^\circ[C \mid Q]] \end{array}$$

Let $J_k = \mathbf{0}$ and $C_k = \overline{\mathit{begin}}\langle u\ n_k\ t_k\ b_k\rangle \mid \varphi_k \mid J_k$. By construction, $C \mid C_k$ is an internal state with an additional session at index k. Let

$$F[\text{-}] \quad \stackrel{\triangle}{=} \quad \nu d_k, sv_k.(\overline{c}\langle d_k, sv_k, SI_k, u, n_k, t_k, b_k\rangle \mid [\text{-}])$$

Using structural equivalences, we obtain $Q \equiv F[C_k]$, $\mathcal{Q}^\circ[C \mid Q] \equiv F[\mathcal{Q}^\circ[C \mid C_k]]$, and finally $A' \equiv E'[P \mid F[\mathcal{Q}^\circ[C \mid C_k]]]$, which is a valid state.

(b) We have a valid state A such that:

$$\begin{array}{rcl} A & \equiv & E'[\overline{s}\langle sv, si, u', n, t, b\rangle.P \mid \mathcal{Q}^\circ[C]] \\ Q & = & \mathit{filter}\ \mathit{checkEvidence}(sv, si, u', s_{pwd}, n, t, b) \mapsto \varnothing\ \mathit{in}\ \overline{\mathit{end}}\langle u'\ n\ t\ b\rangle \\ A' & \equiv & E'[P \mid \mathcal{Q}^\circ[C \mid Q]] \end{array}$$

We first use structural equivalence to close the process Q: we have $A' \equiv E''[\sigma' \mid \mathcal{Q}^\circ[C \mid Q]]$ valid state, for some evaluation context $E''[\text{-}]$ that does not contain any active substitution, and thus $A' \equiv E''[\sigma' \mid \mathcal{Q}^\circ[C \mid Q\sigma]]$ for some $\sigma \equiv \sigma' \mid \sigma_C$.

Applying Lemma 1, we obtain

$$Q\sigma \quad \in \quad \bigoplus\{\overline{end}\langle u' \ n \ t \ b\rangle\sigma \mid \models \mathit{checkEvidence}(sv, si, u', s_{pwd}, n, t, b)\sigma\}$$

Applying Lemma 7, either there exists $i < n$ such that $(u', sv, si, n, t, b = u, sv_i, SI_i, n_i, t_i, b_i)\sigma$, and then $Q\sigma \in \bigoplus\{\overline{end}\langle u \ n_i \ t_i \ b_i\rangle\sigma\}$, or the predicate is never satisfied, and $Q\sigma \in \bigoplus\{\}$.

In the first subcase (the message may be accepted), we let $C' = C \mid Q$, check that C' is an internal state obtained from C by using $J'_i = J_i \mid Q$ instead of J_i, and conclude with $A' \equiv E''[\sigma' \mid \mathcal{Q}^\circ[C \mid Q\sigma]]$, which is a valid state.

In the second subcase (*checkEvidence* fails), let $Q' \in \bigoplus\{\}$ with $Q\sigma \sim Q'$ and $s_{pwd} \notin \mathit{fn}(Q')$ (obtained for instance by substituting a fresh name for s_{pwd} in Q). We have $A' \sim E''[\sigma' \mid Q' \mid \mathcal{Q}^\circ[C]]$, which is a valid state with the same internal state.

(4) The communication entirely occurs in $E[\text{-}]$: we have a valid state A such that:

$$A \equiv E'[A_1 \mid \mathcal{Q}^\circ[C]] \qquad A_1 \mid \sigma_C \rightarrow A'_1 \mid \sigma_C \qquad A' \equiv E'[A'_1 \mid \mathcal{Q}^\circ[C]]$$

Moreover, $s_{pwd} \notin A_1$ by hypothesis on E', so we can pick A''_1 such that $A'_1 \mid \sigma_C \equiv A''_1 \mid \sigma_C$ and $s_{pwd} \notin A''_1$. We conclude with $A' \equiv E'[A''_1 \mid \mathcal{Q}^\circ[C]]$ valid state.

Next, we consider comparison steps. Two cases are enabled, depending on the location of the conditional:

- The test occurs in $\mathcal{Q}^\circ[C]$, necessarily in one of the internal choices: this is another instance of case 1.
- The test occurs in $E[\text{-}]$: this is another instance of case 4. □

As a corollary, we can show robust safety for the core protocol.

Lemma 9 (Core Robust Safety) $\mathcal{Q}^\circ$ *is robustly safe.*

Proof We first show that, if $A \triangleright \overline{a}\langle V\rangle$ and a is used only for asynchronous outputs in A, then $A \rightarrow^* \overline{a}\langle V\rangle \mid A'' \approx A$ for some A''. By definition, $A \triangleright \overline{a}\langle V\rangle$ means $A \approx \overline{a}\langle V\rangle \mid A'$ for some A'. Let $C = \overline{t}\langle\rangle \mid a(x).\mathit{if}\ x = V\ \mathit{then}\ t()$ for some fresh name t. We have $C \mid \overline{a}\langle V\rangle \mid A' \rightarrow^3 A'$ and thus, by context closure and simulation for $\approx$, $C \mid A \rightarrow^* A'' \approx A'$ for some A''. By definition of C and case analysis on reductions, we obtain $A \rightarrow^* \overline{a}\langle V\rangle \mid A''$. By context closure for $\overline{a}\langle V\rangle$, $A'' \approx A'$ implies $\overline{a}\langle V\rangle \mid A'' \approx A$.

Assume $E[\mathcal{Q}^\circ] \rightarrow^* A \triangleright \overline{end}\langle V\rangle$ for some context E[-] where *begin* and *end* do not occur. Using the remark above, we have $E[\mathcal{Q}^\circ] \rightarrow^* A \rightarrow^* B \approx A$ for some $B = \overline{end}\langle V\rangle \mid A''$. By Lemma 8 and induction on the number of reduction steps, there exists a valid state $B' \sim B$. In particular, B' contains a message $\overline{end}\langle V\rangle$. By definition of valid states, this message may occur only within some session state I_i that also contains $\overline{begin}\langle V\rangle$. Thus, $B' \triangleright \overline{begin}\langle V\rangle$ and, since $B' \approx B \approx A$, we obtain $A \triangleright \overline{begin}\langle V\rangle$. □

Theorem 1 follows as a corollary. More generally, we could derive robust safety for configurations that may use several kinds of safe envelopes.

Restatement of Theorem 1 *For any safe envelope, the configuration $\mathcal{Q}$ is robustly safe.*

Proof By Lemma 9, $\mathcal{Q}^\circ$ is robustly safe (RS). By Lemma 5, $\mathcal{Q}^\bullet \approx E_\mathcal{Q}[\mathcal{Q}^\circ]$ and, by hypothesis on $E_\mathcal{Q}$, $E_\mathcal{Q}[\mathcal{Q}^\circ]$ is RS. By Lemma 2, $\mathcal{Q}^\bullet$ is RS. Finally, $\mathcal{Q}^\bullet$ is logically equivalent to $\mathcal{Q}$, and thus, by Lemma 3, $\mathcal{Q}$ is RS. □

4.5 Extended Configurations

In the proofs above, we focused on a simple situation with a single user and a single server dedicated to that user. Next, we illustrate how this basic result can be easily extended to configurations with multiple users and servers.

We first state a lemma to compose robust safety properties.

Lemma 10

(1) *If A is robustly safe and E[-] is an evaluation context where begin and end do not occur, then $E[A]$ is robustly safe.*

(2) *Let A be a process where begin and end do not occur. If $\nu c.A\{a, b = \mathit{begin}, \mathit{end}\}$ and $\nu a.A\{b, c = \mathit{begin}, \mathit{end}\}$ are robustly safe, then $\nu b.A\{a, c = \mathit{begin}, \mathit{end}\}$ is robustly safe.*

Proof

(1) By definition and composition of evaluation contexts.

(2) Assume $E[\nu b.A\{a, c = \mathit{begin}, \mathit{end}\}] \rightarrow^* B \triangleright \overline{end}\langle V\rangle$, and $\mathit{begin}, \mathit{end}, a, b, c$ do not occur in E[-] or V (up to a renaming of a, b, c in A). We also have $E[A] \rightarrow^* B' \triangleright \overline{c}\langle V\rangle$ with $B \equiv \nu b.B'\{a, c = \mathit{begin}, \mathit{end}\}$. Using the second, then the first hypothesis, we also have $B' \triangleright \overline{b}\langle V\rangle$ and $B' \triangleright \overline{a}\langle V\rangle$, and finally $B \triangleright \overline{begin}\langle V\rangle$. □

Theorem 3 *Let $\mathcal{U}$ be a set of variables and Envelope be a family of safe envelopes indexed by $\mathcal{U}$. The configuration $\mathcal{Q}_\mathcal{U} \triangleq \prod_{u\in\mathcal{U}} \mathcal{Q}$ is robustly safe.*

Proof Assume $E[\mathcal{Q}_{\mathcal{U}}] \rightarrow^* B \triangleright \overline{end}\langle V\rangle$ for some evaluation context $E[\text{-}]$ that does not contain *begin*, *end*. Let $\{begin_u, end_u \mid u \in \mathcal{U}\}$ be distinct channel names that do not occur in $E[\text{-}]$. We define renamings $\rho_u \triangleq \{begin_u, end_u = begin, end\}$ and $\rho \triangleq \prod_{u\in\mathcal{U}} \rho_u$, and let $\mathcal{Q}'$ be the configuration $\prod_{u\in\mathcal{U}}(\mathcal{Q}\rho_u^{-1})$. By definition, $\mathcal{Q}_{\mathcal{U}}$ is obtained from $\mathcal{Q}'$ by identifying event channels for all users, and we have $\mathcal{Q}_{\mathcal{U}} = \mathcal{Q}'\rho$.

Event channels appear in $\mathcal{Q}_{\mathcal{U}}$ only for sending messages, and do not appear in $E[\text{-}]$, hence every reduction step in $E[\mathcal{Q}_{\mathcal{U}}] \rightarrow^* B$ commutes with our renamings. We obtain $E[\mathcal{Q}'] \rightarrow^* B' \triangleright \overline{end_u}\langle V\rangle$ for some $u \in \mathcal{U}$ and B' such that $B = B'\rho$, and finally $E[\mathcal{Q}'\rho_u] \rightarrow^* B'\rho_u \triangleright \overline{end}\langle V\rangle$.

By Theorem 1 and Lemma 10(1), the configuration $E[\mathcal{Q}'\rho_u]$ is robustly safe, hence $B'\rho_u \triangleright \overline{end}\langle V\rangle$ implies $B'\rho_u \triangleright \overline{begin}\langle V\rangle$ and, since $B = B'\rho$, $B \triangleright \overline{begin}\langle V\rangle$. □

To see that this indeed allows us to consider systems with multiple users, using structural equivalence, we have $\mathcal{Q}_{\mathcal{U}} \equiv \nu(s_u)_{u\in\mathcal{U}}.(I \mid S)$ where $I \triangleq \prod_{u\in\mathcal{U}}(\{u = \mathsf{principal}(s_u)\} \mid I_u)$ implements a parallel composition of initiators for the users in $\mathcal{U}$ (all using distinct passwords) and $S \triangleq \prod_{u\in\mathcal{U}} S_u$ implements a server that accepts requests from any of these users (with an internal choice of $u \in \mathcal{U}$ as each envelope is received). Similarly, we could extend our result to initiators using multiple safe envelope formats for a given user.

In our configurations so far, whenever the server accepts a message, it only sends an end-event. The next lemma extends robust safety in case the server performs some additional processing on accepted messages. (This lemma can be used as a preliminary step before chaining sub-protocols using Lemma 10; see also Section 4.7 for an application.)

Lemma 11 *The configuration $\mathcal{Q}'$ obtained from $\mathcal{Q}$ by substituting $\mathcal{Q}[\overline{end}\langle u'\ n\ t\ b\rangle \mid \overline{accept}\langle u', n, t, b\rangle]$ for $\mathcal{Q}[\overline{end}\langle u'\ n\ t\ b\rangle]$ is robustly safe.*

Proof Using robust safety for $\mathcal{Q}$ (Theorem 1), whenever a message is sent on *end*, we have $u = u'$ and the values n, t, b are those received from the environment on $init_u$. By mapping reductions $E[\mathcal{Q}'] \rightarrow^* A$ to those of $E'[\mathcal{Q}]$ where E' is $E[\text{-}]$ plus messages on *accept*, we easily establish that $E[\mathcal{Q}']$ is also safe. □

4.6 Stating and Proving X.509-Based Authentication

For expressing X.509 configurations, we model the certifier as a process $A_{\mathcal{I}}$ that exports its own public key k_r plus a collection of certificates for the pairs of users and public keys $(V, K) \in \mathcal{I}$, signed with the certifying private key, s_r. The configuration also includes client and server processes for a particular user u, with public key k_u.

X.509 Signing Protocol Configurations: $\mathcal{Q}$ (parameterized by $Envelope, \mathcal{I}$)

$$\begin{aligned}
\mathcal{Q} &\triangleq A_{\mathcal{I}} \mid K_u \mid S_u \\
A_{\mathcal{I}} &\triangleq \nu s_r.\Big(\{k_r = \mathsf{pk}(s_r)\} \mid \textstyle\prod_{(V,K)\in\mathcal{I}}\{x_V = \mathsf{x509}(s_r, V, \mathtt{rsa\text{-}sha1}, K)\}\Big) \\
K_u &\triangleq \nu s_u.(\{u = \mathsf{principal}(s_u)\} \mid \{k_u = \mathsf{pk}(s_u)\} \mid I_u)
\end{aligned}$$

$$
\begin{array}{lcl}
I_u & \triangleq & !init_u(b, ea, et, ei).(\overline{begin}\langle u\ b\ ea\ et\ ei\rangle \mid \overline{http}\langle Envelope\rangle) \\
S_u & \triangleq & !http(e). \\
 & & \mathit{filter}\ hasX509SignedBody(e, k_r, u,\ W, S, id, b, ea, et, ei) \mapsto id, b, ea, et, ei\ \mathit{in} \\
 & & \overline{end}\langle u\ b\ ea\ et\ ei\rangle
\end{array}
$$

As in Section 4, the configuration $\mathcal{Q}$ illustrates a simple protocol configuration. Its definition can easily be adapted to deal with more general configurations. We make the following assumptions on the contents of certificates and envelopes:

Safe Collections of Certificates: $\mathcal{I}$

$\mathcal{I}$ is a finite set of pairs of terms such that, whenever $(V, K) \in \mathcal{I}$, either $(V, K) = (u, k_u)$, or $fv(V, K) = \varnothing$ and $s_r \notin fn(V, K)$.

These conditions guarantee that there is a unique certificate for u and k_u, and that the certifying key is used exclusively for signing these certificates.

Safe Envelopes with X.509 Signing:

A *safe envelope* is a term of the form $Envelope = T\varphi$ for any terms T and SI such that $s_r, s_u \notin fn(T) \cup fn(SI)$ and $isSigInfo(SI, \texttt{rsa-sha1}, b, ea, et, ei)$ is valid, with the active substitution φ defined by:

$$\varphi \quad \triangleq \quad \{sv = \mathsf{rsa\text{-}sha1}(\mathsf{c14n}(SI), s_u)\}$$

The structure of the proof is similar to the one detailed in Section 4.4. We first decompose $hasX509SignedBody(e, k_r, u, ac, to, id, b, ea, et, ei) \mapsto id, b, ea, et, ei$ into the conjunction

$$
\begin{array}{l}
hasX509SignatureEvidence(e, id, x, sv, si, b, ea, et, ei) \mapsto id, x, sv, si, b, ea, et, ei, \\
checkX509Evidence(k_r, u, ac, to, id, x, sv, si, b, ea, et, ei) \mapsto \varnothing
\end{array}
$$

Here, *checkX509Evidence* contains all the cryptographic tests to check the certificate and the signature:

$$
\begin{array}{l}
checkX509Evidence(k_r : \mathsf{bytes}, u, ac, to, id : \mathsf{string}, x, sv : \mathsf{bytes}, si, b, ea, et, ei : \mathsf{item}) \texttt{ :-} \\
\quad isX509Cert(x, k_r, u, \texttt{rsa-sha1}, k), \\
\quad isSigVal(sv, si, k, \texttt{rsa-sha1}), \\
\quad isSigInfo(si, \texttt{rsa-sha1}, b, ea, et, ei), \\
\quad ea = \texttt{<action \_>}ac\texttt{</>}, \\
\quad et = \texttt{<to \_>}to\texttt{</>}, \\
\quad ei = \texttt{<id \_>}id\texttt{</>}.
\end{array}
$$

$$
\begin{array}{l}
isX509Cert(x, k_r : \mathsf{bytes}, u, a : \mathsf{string}, k : \mathsf{bytes}) \texttt{ :-} \\
\quad \mathsf{check\text{-}x509}(x, k_r) = k_r, \\
\quad u = \mathsf{x509\text{-}user}(x), \\
\quad a = \mathsf{x509\text{-}alg}(x), \\
\quad k = \mathsf{x509\text{-}key}(x).
\end{array}
$$

Next, we define core protocol configurations and their valid states.

X.509 Signing Core Protocol Configurations: $\mathcal{Q}^\circ$ (parameterized by SI, $\mathcal{I}$)

$$
\begin{array}{rcl}
\mathcal{Q}^\circ[\text{-}] & \triangleq & A_{\mathcal{I}} \mid K_u^\circ \mid S_u^\circ \mid [\text{-}] \\
K_u^\circ & \triangleq & \nu s_u.(\{u = \mathsf{principal}(s_u)\} \mid \{k_u = \mathsf{pk}(s_u)\} \mid I_u^\circ) \\
I_u^\circ & \triangleq & !init_u(b, ea, et, ei).(\overline{begin}\langle u\ b\ ea\ et\ ei\rangle \mid \\
 & & \qquad \overline{c}\langle \mathtt{id}.\mathsf{Body}(ei), x_u, sv, SI, b, ea, et, ei\rangle) \\
S_u^\circ & \triangleq & !s(id, x, sv, si, b, ea, et, ei). \\
 & & filter\ checkX509Evidence(k_r, u, W, S, id, x, sv, si, b, ea, et, ei) \mapsto \varnothing\ in \\
 & & \overline{end}\langle u\ b\ ea\ et\ ei\rangle
\end{array}
$$

Valid States for the X.509 Signing Protocol:

(1) φ_i is adapted from φ in the definition of safe envelopes with variables $sv_i, b_i, ea_i, et_i, ei_i$ and term SI_i instead of sv, b, ea, et, ei and SI.

(2) A *session state* is a process of the form $C_i = \overline{begin}\langle u\ b_i\ ea_i\ et_i\ ei_i\rangle \mid \varphi_i \mid J_i$ where J_i is any parallel composition of processes from $\{\overline{end}\langle u\ b_i\ ea_i\ et_i\ ei_i\rangle\} \cup \bigoplus\{\overline{end}\langle u\ b_i\ ea_i\ et_i\ ei_i\rangle\} \cup \bigoplus\{\}$. ($C_i$ has free variables b_i, ea_i, et_i, ei_i and defined variable sv_i.)

(3) An *internal state* is a parallel composition of session states $C = \prod_{i<m} C_i$, for some $m \geq 0$.

(4) A *valid state* is a closed process of the form $A = E[\mathcal{Q}^\circ[C]]$ where $E[\text{-}]$ is an evaluation context where *begin* and *end* do not occur and C is an internal state.

For a given internal state C, let σ_C^1 be the (ordinary) substitution obtained by composing $\{k_r = \mathsf{pk}(s_r)\}$ and each $\{x_V = \mathsf{x509}(s_r, V, \mathtt{rsa\text{-}sha1}, K)\}$ for $(V, K) \in \mathcal{I}$; let σ_C^2 be obtained by composing $\{u = \mathsf{principal}(s_u)\}, \{k_u = \mathsf{pk}(s_u)\}$ and each φ_i for $i < m$. Let $\sigma_C = \sigma_C^1 \mid \sigma_C^2$. By definition, the frame obtained from $\mathcal{Q}^\circ[C]$, which represents the attacker's knowledge about s_u, is $\varphi_C = \nu s_r.\sigma_C^1 \mid \nu s_u.\sigma_C^2$.

We prove the safety of *checkX509Evidence* in two steps: first we show that the certificate scheme is safe, Lemma 13, and then we show that the signature scheme is safe, Lemma 14. Both proofs are reminiscent of the proof of Lemma 7. The first lemma in our development states some facts about our equational theory.

Lemma 12 (Normal Forms with Certificates)

(1) *Let σ be a substitution ranging over two forms of terms: either $\mathsf{pk}(s_r)$, or $\mathsf{x509}(s_r, V_1, V_2, V_3)$ with $s_r \notin fn(V_1, V_2, V_3)$ and $dom(\sigma) \cap (fv(V_1, V_2, V_3)) = \varnothing$.*

For each U in normal form with $s_r \notin fn(U)$, there exists U' with $s_r \notin fn(U')$, $U'\sigma = U\sigma$, and $U'\sigma$ in normal form.

(2) *Let σ be a substitution ranging over two forms of terms: either $\mathsf{pk}(s_u)$, or $\mathsf{rsa\text{-}sha1}(V, s_u)$ with $s_u \notin fn(V)$.*

For each U in normal form with $s_u \notin fn(U)$, there exists U' with $s_u \notin fn(U')$, $U'\sigma = U\sigma$, and $U'\sigma$ in normal form.

Proof We prove the two parts in a similar fashion. As before, we write $U \mapsto V$ for the reduction relation obtained by orienting our equations on terms from left to right, and closing under contexts.

(1) Suppose $U\sigma$ reduces by a sequence of rewrite steps to V. We write $\mapsto$ for a rewrite step; so, $U\sigma \mapsto^n V$. We prove, by induction on the number of rewrite steps n, that V is of the form $U'\sigma$ such that $s_r \notin fn(U')$. As a corollary, if V is the normal form of $U\sigma$, then there exists U' in normal form, $s_r \notin fn(U')$, such that $U'\sigma$ is V.

Base case: $U\sigma$ is V, so, let U' be U.

Inductive hypothesis: $U\sigma \mapsto^k U_k\sigma$, $s_r \notin fn(U_k)$, and $U_k\sigma \mapsto V$. Then, $U_k\sigma$ is $C[L\tau]$ and V is $C[R\tau]$ where $L \mapsto R$ is a rewrite rule. So, U_k is $C'[L']$, such that C is $C'\sigma$ and $L'\sigma$ is $L\tau$. If L' matches L (L' is $L\mu$), then the redex occurs in U_k itself and V is $U_{k+1}\sigma$, where $U_k \mapsto U_{k+1}$; so, let U' be U_{k+1}. Otherwise, $L'\sigma$ matches L but L' does not. By case analysis on rewrite rules ($L \rightarrow_{\mathcal{R}} R$), we find all such L':

- L' is $\mathsf{x509\text{-}user}(x)$ and $\sigma(x)$ is $\mathsf{x509}(s_r, V_1, V_2, V_3)$, $s_r \notin fn(V_1, V_2, V_3)$, $x \notin fv(V_1, V_2, V_3)$. Then $C[L'\sigma] \mapsto C[V_1]$, that is $C'\sigma[V_1]$, that is $(C'[V_1])\sigma$ (since $x \notin fv(V_1)$. So, let U' be $C'[V_1]$.
- L' is $\mathsf{x509\text{-}alg}(x)$ and $\sigma(x)$ is $\mathsf{x509}(s_r, V_1, V_2, V_3)$, $s_r \notin fn(V_1, V_2, V_3)$, $x \notin fv(V_1, V_2, V_3)$. Same as previous case, with V_2 instead of V_1. So, let U' be $C'[V_2]$.
- L' is $\mathsf{x509\text{-}key}(x)$ and $\sigma(x)$ is $\mathsf{x509}(s_r, V_1, V_2, V_3)$, $s_r \notin fn(V_1, V_2, V_3)$, $x \notin fv(V_1, V_2, V_3)$. Same as previous case, with V_3 instead of V_2. So, let U' be $C'[V_3]$.
- L' is $\mathsf{check\text{-}x509}(\_, y)$, $\sigma(y)$ is $\mathsf{pk}(s_r)$. Then $C[L'\sigma] \mapsto C[\mathsf{pk}(s_r)]$, that is $(C'[y])\sigma$. So, let U' be $C'[y]$.
- L' is $\mathsf{check\text{-}rsa\text{-}sha1}(\_, \_, y)$, $\sigma(y)$ is $\mathsf{pk}(s_r)$. Then $C[L'\sigma] \mapsto C[\mathsf{pk}(s_r)]$, that is $(C'[y])\sigma$. So, let U' be $C'[y]$.
- In all other cases, if $L'\sigma$ matches L, so does L'.

(2) Suppose $U\sigma \mapsto^n V$. Again, we prove, by induction on the number of rewrite steps n, that V is of the form $U'\sigma$ such that $s_u \notin fn(U')$. As a corollary, if V is the normal form of $U\sigma$, then there exists U' in normal form, $s_u \notin fn(U')$, such that $U'\sigma$ is V.

Base case: $U\sigma$ is V, so, let U' be U.

Inductive hypothesis: $U\sigma \mapsto^k U_k\sigma$, $s_u \notin fn(U_k)$, and $U_k\sigma \mapsto V$. Then, $U_k\sigma$ is $C[L\tau]$ and V is $C[R\tau]$ where $L \mapsto R$ is a rewrite rule. So, U_k is $C'[L']$, such that C is $C'\sigma$ and $L'\sigma$ is $L\tau$. If L' matches L (L' is $L\mu$), then the redex occurs in U_k itself and V is $U_{k+1}\sigma$, where $U_k \mapsto U_{k+1}$; so, let U' be U_{k+1}.

Otherwise, $L'\sigma$ matches L but L' does not. By case analysis on rewrite rules ($L \rightarrow_{\mathcal{R}} R$), we find all such L':

- L' is $\mathsf{check\text{-}x509}(\_, y)$, $\sigma(y)$ is $\mathsf{pk}(s_u)$. Then $C[L'\sigma] \mapsto C[\mathsf{pk}(s_u)]$, that is $(C'[y])\sigma$. So, let U' be $C'[y]$.
- L' is $\mathsf{check\text{-}rsa\text{-}sha1}(\_, \_, y)$, $\sigma(y)$ is $\mathsf{pk}(s_u)$. Then $C[L'\sigma] \mapsto C[\mathsf{pk}(s_u)]$, that is $(C'[y])\sigma$. So, let U' be $C'[y]$.
- In all other cases, if $L'\sigma$ matches L, so does L'. □

Lemma 13 (*isX509Cert* is safe) *Let C be an internal state with $m \geq 0$ sessions. Let σ' be a substitution that ranges over open terms where the name s_r does not appear such that $\sigma \triangleq \sigma' \mid \sigma^1_C$ is closed. Let $\mathcal{I}$ be a safe collection of certificates. If*

$$\models \mathit{isX509Cert}(x, k_r, w, \mathit{rsa\text{-}sha1}, k)\sigma$$

then there exists $(V, K) \in \mathcal{I}$ such that $(x, w, k = x_v, V, K)\sigma$.

Proof Assume $\models \mathit{isX509Cert}(x, k_r, w, \mathsf{rsa\text{-}sha1}, k)\sigma$ and let σ°_C be such that $\sigma = \sigma' \mid \sigma^\circ_C$ and σ°_C ranges over closed terms in normal forms. Hence, $\mathit{dom}(\sigma^\circ_C) = \mathit{dom}(\sigma^1_C) = \{k_r\} \cup \{x_V \mid (V, K) \in \mathcal{I}\}$ and, for all $x \in \mathit{dom}(\sigma_C)$, $x\sigma^\circ_C = x\sigma^1_C$.

From the definition of *isX509Cert*, and rewriting for k_r, we get:

$$\models (\mathsf{check\text{-}x509}(x, \mathsf{pk}(s_r)) = \mathsf{pk}(s_r))\sigma \tag{7}$$

$$\models (w = \mathsf{x509\text{-}user}(x))\sigma \tag{8}$$

$$\models (k = \mathsf{x509\text{-}key}(x))\sigma \tag{9}$$

Let N be the normal form of $x\,\sigma$. From (7), we get $\mathsf{check\text{-}x509}(N, \mathsf{pk}(s_r)) = \mathsf{pk}(s_r)$, with both terms in normal form. Using Lemma 6(5), cases (a) and (c) can be eliminated, since $\mathsf{check\text{-}x509} \neq \mathsf{pk}$ and pk is a constructor. So only case (b) applies: $\mathsf{check\text{-}x509}(N, \mathsf{pk}(s_r))$ is a redex, and must match the (only) rule for $\mathsf{check\text{-}x509}$: $N = \mathsf{x509}(s_r, u', a', k')$, that is $x\,\sigma = \mathsf{x509}(s_r, u', a', k')$.

Let $T = x\,\sigma'$ in normal form; so, $s_r \notin \mathit{fn}(T)$ and $x\,\sigma = T\,\sigma^\circ_C$. From the assumptions on $\mathcal{I}$, we have that the range of σ°_C consists of $\mathsf{pk}(s_r)$ and terms of the form $\mathsf{x509}(s_r, V_1, V_2, V_3)$, such that $s_r \notin \mathit{fn}(V_1, V_2, V_3)$ and $\mathit{dom}(\sigma^\circ_C) \cap \mathit{fv}(V_1, V_2, V_3) = \varnothing$. Using Lemma 12(1) and the definition of σ°_C, there exists T' in normal form, such that T' does not contain s_r, $T'\,\sigma^\circ_C = T\,\sigma^\circ_C$, and $T'\,\sigma^\circ_C$ is also in normal form.

So, $T'\,\sigma^\circ_C = x\,\sigma = \mathsf{x509}(s_r, u', a', k')$, and by plain structural matching on normal forms, we obtain three cases for T:

- $T = y$ for some $y \in \mathit{dom}(\sigma^\circ_C)$ such that $y\,\sigma^\circ_C = \mathsf{x509}(s_r, \_, \_, \_)$, where $\_$ stands for any subterm.
  By definition of σ°_C, this implies $y = x_V$ for some $(V, K) \in \mathcal{I}$, and thus $(x = x_V)\sigma$.

- $T = \mathsf{x509}(y, \_)$ for some $y \in \mathit{dom}(\sigma^\circ_C)$ such that $y\,\sigma^\circ_C = s_r$.
  This is excluded by definition of σ°_C.

- $T = \mathsf{x509}(s_r, \_)$.
  This is excluded by hypothesis on σ': since $T = x\,\sigma'$, we have $s_r \notin \mathit{fn}(T)$.

So $(x = x_V)\sigma$, for $(V, K) \in \mathcal{I}$. Using (8), 9, and the definition of x_V in σ°_C, we obtain $(w, k = V, K)\sigma$. □

Lemma 14 (*checkX509Evidence* is safe) *Let C be an internal state with $m \geq 0$ sessions. Let σ' be a substitution that ranges over open terms where the names s_r, s_u do not appear such that $\sigma \triangleq \sigma' \mid \sigma^1_C \mid \sigma^2_C$ is closed. Let $\mathcal{I}$ be a safe collection of certificates. If*

$$\models \mathit{checkX509Evidence}(k_r, u, W, S, x, sv, si, b, ea, et, ei)\sigma$$

then there exists $i < n$ such that $(sv, si, b, ea, et, ei = sv_i, SI_i, b_i, ea_i, et_i, ei_i)\sigma$.

Proof Assume $\models \mathit{checkX509Evidence}(k_r, u, W, S, x, sv, si, b, ea, et, ei)\sigma$ and let σ°_C be such that $\sigma = \sigma' \mid \sigma^1_C \mid \sigma^\circ_C$ and σ°_C ranges over closed terms in normal forms.

Then, by definition of $\models$, there exists σ'' with $\mathit{dom}(\sigma'') = \{k, \mathit{auri}, \mathit{turi}\}$ such that:

$$\models \mathit{isX509Cert}(x, k_r, u, \mathsf{rsa\text{-}sha1}, k)\sigma\sigma'' \tag{10}$$

$$\models (sv = \mathsf{rsa\text{-}sha1}(k, \mathsf{c14n}(si)))\sigma\sigma'' \tag{11}$$

$$\models \mathit{isSigInfo}(si, \texttt{rsa-sha1}, b, ea, et, ei)\sigma\sigma'' \tag{12}$$

$$\models (ea = \texttt{<action }\mathit{auri}\texttt{>}S\texttt{</>})\sigma\sigma'' \tag{13}$$

$$\models (et = \texttt{<to }\mathit{turi}\texttt{>}W\texttt{</>})\sigma\sigma'' \tag{14}$$

Using Lemma 13 and (10), we get $(x, u, k = x_V, V, K)\sigma\sigma''$ for some $(V, K) \in \mathcal{I}$. Using the assumption on $\mathcal{I}$, we get $(K = k_u)\sigma$.

In (11), using the definition of k_u in σ^2_C, and normalizing both sides of the equation, we get $\mathsf{check\text{-}rsa\text{-}sha1}(\mathsf{c14n}(si'), sv', \mathsf{pk}(s_u)) = \mathsf{pk}(s_u)$, where si', sv' are normal forms of $si\,\sigma, sv\,\sigma$. Using Lemma 6(5), cases (a) and (c) can be eliminated, since $\mathsf{check\text{-}rsa\text{-}sha1} \neq \mathsf{pk}$ and pk is a constructor. So from case (b), $\mathsf{check\text{-}rsa\text{-}sha1}(\mathsf{c14n}(si'), sv', \mathsf{pk}(s_u))$ must match the (only) rule for $\mathsf{check\text{-}rsa\text{-}sha1}$: $sv' = \mathsf{rsa\text{-}sha1}(\mathsf{c14n}(si'), s_u)$, that is $sv\,\sigma = \mathsf{rsa\text{-}sha1}(\mathsf{c14n}(si'), s_u)$.

Let $T = sv\,\sigma'\,\sigma^1_C$ in normal form; so, $s_u \notin \mathit{fn}(T)$ and $sv\,\sigma = T\,\sigma^\circ_C$.

Using Lemma 12(2) and the definition of σ°_C, $T\,\sigma^\circ_C = T'\,\sigma^\circ_C$, for T' and $T'\,\sigma^\circ_C$ in normal form. So, $T'\,\sigma^\circ_C = \mathsf{rsa\text{-}sha1}(\mathsf{c14n}(si'), s_u)$, with both terms in normal form, and by plain structural matching on normal forms, we obtain three cases for T:

- $T = y$ for some $y \in \mathit{dom}(\sigma^\circ_C)$ such that $y\,\sigma^\circ_C = \mathsf{rsa\text{-}sha1}(\_, s_u)$, where $\_$ stands for any subterm.
  By definition of σ°_C, this implies $y = sv_i$ for some $i < n$, and thus $(sv = sv_i)\sigma$.

- $T = \mathsf{rsa\text{-}sha1}(\_, y)$ for some $y \in \mathit{dom}(\sigma^\circ_C)$ such that $y\,\sigma^\circ_C = s_u$.
  This is excluded by definition of σ°_C.

- $T = \mathsf{rsa\text{-}sha1}(\_, s_u)$.
  This is excluded by hypothesis on σ': since $T = x\,\sigma'$, we have $s_u \notin \mathit{fn}(T)$.

Using the definition of sv_i in σ_C, equation (6) becomes

$$\mathsf{rsa\text{-}sha1}(\mathsf{c14n}(si\,\sigma), s_u) = \mathsf{rsa\text{-}sha1}(\mathsf{c14n}(SI_i\,\sigma), s_u)$$

and thus Lemma 6(4) yields $(si = SI_i)\sigma$.

Similarly, expanding the definition of *isSigInfo* in (12) and in SI_i, we obtain an equation of the form:

$$(W\{x = b\}\{y = ea\}\{z = et\}\{w = ei\} = W\{x = b_i\}\{y = ea_i\}\{z = et_i\}\{w = ei_i\})\sigma$$

for a term W built only from constructors, and obtain $(b, ea, et, ei = b_i, ea_i, et_i, ei_i)\sigma$ from Lemma 6(4). □

Theorem 4 *For any safe Envelope and any safe collection of certificates $\mathcal{I}$, the configuration $\mathcal{Q}$ is robustly safe.*

Proof The proof has the same structure as in Section 4.4. We rely here on a different definition of φ_i and *checkEvidence*, whose correctness is established in Lemma 14. We easily establish the counterpart of Lemma 4

We check that the proofs of Lemmas 8, 9, 5 and the main proof of Theorem 1 apply unchanged to our modified definitions. □

4.7 Stating and Proving Firewall-Based Authentication

For the firewall-based protocol, we define the full protocol configurations as follows.

Firewall Protocol Configurations: $\mathcal{Q}$ (param. by $Envelope_u, Envelope_f, \mathcal{I}$)

$$\begin{array}{rcl}
\mathcal{Q} & \triangleq & A_{\mathcal{I}} \mid \nu init_f.(\nu s_u.(\{u = \mathsf{principal}(s_u)\} \mid I_u \mid S_u^f) \mid K_f^u) \mid S_f \\
A_{\mathcal{I}} & \triangleq & \nu s_r.\Big(\{k_r = \mathsf{pk}(s_r)\} \mid \prod_{(V,K)\in\mathcal{I}}\{x_V = \mathsf{x509}(s_r, V, \mathtt{rsa\text{-}sha1}, K)\}\Big) \\
I_u & \triangleq & !init_u(n,t,b).(\overline{begin}\langle u\ n\ t\ b\rangle \mid \overline{http_u}\langle Envelope_u\rangle) \\
S_u^f & \triangleq & !http_u(e).\ \underline{filter}\ hasUserSignedBody(e,u,s_u,n,t,b) \mapsto n,t,b\ in \\
 & & \qquad \overline{end_u}\langle u\ n\ t\ b\rangle \mid \overline{init_f}\langle u,n,t,b\rangle \\
K_f^u & \triangleq & \nu s_f.(\{f = \mathsf{principal}(s_f)\} \mid \{k_f = \mathsf{pk}(s_f)\} \mid I_f) \\
I_f & \triangleq & !init_f(u,n,t,b).(\overline{begin_f}\langle u\ n\ t\ b\rangle \mid \overline{http_f}\langle Envelope_f\rangle) \\
S_f & \triangleq & !http_f(e).\ \underline{filter}\ hasX509SignedBodyFw(e,k_r,f,u',n,t,b) \mapsto u',n,t,b\ in \\
 & & \qquad \overline{end}\langle u'\ n\ t\ b\rangle
\end{array}$$

This configuration is obtained by merging those of Sections 4.3 and 4.6: up to indexing, I_u and S_f^u are the same as for password-based signature (Section 4.3). $A_{\mathcal{I}}$ is defined as in Section 4.6; K_f^u and I_f^u are similar to K_u and I_u in that section: the main difference is that the originator (u) received on $init_f$ is used instead of the immediate sender (f). S_f is similar to S_u in Section 4.6: they differ mostly in the content of the signature. We adapt the definition of safe X.509-signed envelopes accordingly:

Safe Envelopes with X.509 Signing (Adapted for Firewall):

A *safe envelope* is a term of the form $Envelope_f = T\varphi$ for some terms T, SI, and FW such that $s_r, s_f \notin fn(T) \cup fn(SI)$, $isSigInfo(SI, \texttt{rsa-sha1}, b, FW)$ and $isFirewallHeader(FW, u, n, t)$ are valid, with the active substitution φ defined by:

$$\varphi \;\triangleq\; \{sv = \mathsf{rsa\text{-}sha1}(\mathsf{c14n}(SI), s_u)\}$$

We also adapt the definition of safe collections of certificates to guarantee a unique certificate for (f, k_f) instead of (u, k_u).

Lemma 15 *For any safe envelope and any safe collection of certificates $\mathcal{I}$, the adapted X.509 protocol configuration: $\mathcal{Q}' \triangleq A_{\mathcal{I}} \mid K_f^u\{begin_f = begin\} \mid S_f$ is robustly safe.*

Proof The proof is almost identical to the main proof of Section 4.6; we use variables u, n, t, b instead of b, ea, et, ei to represent arbitrary terms received on $init_f$ then signed. The main difference is in showing that if

- $\models isSigInfo(SI, \texttt{rsa-sha1}, b_1, FW_1)\sigma$, $\models isFirewallHeader(FW_1, u_1, n_1, t_1)$,
- $\models isSigInfo(SI, \texttt{rsa-sha1}, b_2, FW_2)\sigma$, $\models isFirewallHeader(FW_2, u_2, n_2, t_2)$,

then $(b_1, u_1, n_1, t_1 = b_2, u_2, n_2, t_2)\sigma$ □

Lemma 16 *Let ρ be the event renaming $\{begin, end_u, begin_f, end = begin_u, begin, end, end_f\}$. The configuration $\mathcal{Q}\rho$ is robustly safe.*

Proof Let $\mathcal{Q}^\circ$ be $\mathcal{Q}$ with $\overline{init_f}\langle u, n, t, b\rangle$ replaced by the messages $\overline{begin_f}\langle u\ n\ t\ b\rangle \mid \overline{http_f}\langle Envelope_f\rangle$ in S_u^f. Since messages sent on $init_f$ are exclusively received by I_f, we obtain $\mathcal{Q}^\circ \approx \mathcal{Q}$ using a standard observational equivalence in the pi calculus.

We remark that $\mathcal{Q}^\circ\rho \equiv C[\overline{end}\langle u, n, t, b\rangle \mid \overline{begin}\langle u, n, t, b\rangle]$ for some context $C[\text{-}]$ where the channels *begin* and *end* do not occur, and easily establish that any configuration with this structural property is robustly safe. □

Theorem 5 *For any safe envelopes $(Envelope_u, Envelope_f)$ for password-based signing and adapted X.509 signing, respectively, and for any certificates safe collection of certificates $\mathcal{I}$, the configuration $\nu end_u, begin_f.\mathcal{Q}$ is robustly safe.*

Proof Relying on Lemma 10, we compose Lemma 11 with the renaming $\{accept = init_f\}$ in evaluation context, Lemma 16, and Lemma 15 in evaluation context. □

5 Conclusions and Future Work

In this paper, we introduced a framework for reasoning about the security of SOAP protocols and their cryptographic implementations in terms of WS-Security tokens. We illustrated our framework using a series of simple authentication protocols. Surprisingly, perhaps, these XML-based protocols can be studied at the same (syntactic) level of abstraction:

- formally, using a faithful, predicate-based implementation in the applied pi calculus with proofs of correspondence properties against a Dolev-Yao adversary;
- experimentally, using sample programs and SOAP traces on top of the WSE toolkit [29].

This should provide a principled basis for testing compliant implementations, and also reduce the risk of attacks in concrete refinements of correct, abstract protocols.

As can be expected, this also complicates the formal model, with for example a large syntax and equational theory for terms in the applied pi calculus. However, our experience suggests that a modular definition of predicates, together with standard compositional techniques in the pi calculus, should enable a good reuse of the proof effort for numerous WS-Security protocols.

Our choice of authentication protocols stresses that small variations in WS-Security envelope formats may lead to much weaker correspondence properties. Each service should therefore clearly prescribe (and enforce) the intended property. Specifically, a prudent practice in the selection of XML signatures is to request that all potentially relevant headers be jointly authenticated—not just the message identifier or its body. In the case authentication relies on username tokens, this strongly suggests the use of a signature instead of a digest. Moreover, XML signatures have a complex structure, which should be used with caution. Specifically, authentication should not rely on signed elements whose interpretation depends on an unsigned context.

5.1 Related Work

There have been many formal studies of remote procedure call (RPC) security mechanisms. The earliest we are aware of is the formalization within the BAN logic [10] of Secure RPC [36] in the Andrew distributed computing environment. More recently, process calculi [2] have been used to formalize the secure implementation of programming abstractions such as communication channels and network objects [39].

We are aware of very little prior formal work on XML security protocols. Gordon and Pucella [22] implement and verify attribute-driven SOAP-level security protocols, but do not use the WS-Security syntax. Their representation of SOAP messages abstracts many details of the XML wire format, and hence would be blind to any errors in the detailed structure of names or signatures. Damiani *et al.* [13] describe an access control model for SOAP messages, but rely on a secure transport rather than WS-Security; a subsequent paper [14] discusses connections between SOAP security and authorization languages such as SAML and XACML.

5.2 Future Work

Our approach to authenticity properties should extend to complementary security properties, such as secrecy and anonymity. Similarly, we should be able to deal with more complex protocols (with series of related messages) and configurations (with more principals and roles). Our predicate structure is quite modular, with predicates being re-used in different protocols. Hence, we are hopeful that the method will scale up. Moreover, our semantics appears to be suitable for automation, and we are investigating how to automate the proofs using Blanchet's recent logic-based tool for applied pi [6].

At this stage, we are exploring the range of WS-Security protocols, rather than attempting its thorough description. Our fragment of WS-Security omits certain features and options such as encryption, Kerberos tokens, and XPath transforms, but we see no fundamental barrier to modelling all of the specification.

Finally, although all the protocols are implemented using WSE, our goal has not been to verify the WSE implementation itself. There is an informal gap between our formal model and the actual implementation: we have not mechanically checked that our predicates correspond correctly to the checks made by WSE. Still, we are investigating ways of verifying at least parts of the implementation by relating it to our semantics.

Acknowledgements We thank Tony Hoare, Riccardo Pucella, and anonymous reviewers for their comments.

A The Applied Pi Calculus (Overview)

The applied pi calculus is a simple, general extension of the pi calculus with value passing, primitive function symbols, and equations between terms. Abadi and Fournet [1], introduce this calculus, develop semantics and proof techniques, and apply those techniques in reasoning about some security protocols. This appendix gives only a brief overview derived from [20].

In the applied pi calculus, the constructs of the classic pi calculus can be used to represent concurrent systems that communicate on channels, and function symbols can be used to represent cryptographic operations and other operations on data. Large classes of important attacks can also be expressed in the applied pi calculus, as contexts. These include the typical attacks for which a symbolic, mostly "black-box" view of cryptography suffices (but not for example some lower-level attacks that depend on timing behaviour or dictionary attacks). Some of the properties of the protocol can be nicely captured in the form of equivalences between processes. Moreover, some of the properties are sensitive to the equations satisfied by the cryptographic functions upon which the protocol relies. The applied pi calculus is well-suited for expressing those equivalences and those equations.

Abstractly, a *signature* Σ consists of a finite set of function symbols, such as concat and sha1, each with an integer arity. Given a signature Σ, an infinite set of names, and an infinite set of variables, the set of *terms* is defined by the grammar:

Grammar for Terms:

$T, U, V, SI, \mathit{Envelope} ::=$	terms
$\mathit{begin}, \mathit{end}, \mathit{http}, \mathit{init}, c, s$	name (for communication channels)
s_{pwd}, s_r, s_u	name (for cryptographic secrets)
b, e, n, x, y, t, u	variable
$f(T_1, \ldots, T_l)$	function application

where f ranges over the function symbols of Σ and l matches the arity of f. We use metavariables v and w to range over both names and variables.

The grammar for *processes* is similar to the one in the pi calculus, except that messages can contain terms (rather than only names) and that names need not be just channel names:

Grammar for Processes:

$P, Q, R ::=$	processes (or plain processes)
$\mathbf{0}$	null process
$P \mid Q$	parallel composition
$!P$	replication
$\nu s.P$	name restriction ("new")
$\mathit{if}\ U = V\ \mathit{then}\ P\ \mathit{else}\ Q$	conditional
$v(x).P$	message input
$\overline{v}\langle T\rangle.P$	message output

The null process $\mathbf{0}$ does nothing; $P \mid Q$ is the parallel composition of P and Q; the replication $!P$ behaves as an infinite number of copies of P running in parallel. The process $\nu s.P$ makes a new name s then behaves as P. The conditional construct *if* $U = V$ *then* P *else* Q is standard, but we should stress that $U = V$ represents equality in the equational theory, rather than strict syntactic identity. We abbreviate it *if* $U = V$ *then* P when Q is $\mathbf{0}$. Finally, the input process $v(x).P$ is ready to input from channel v, then to run P with the actual message replaced for the formal parameter x, while the output process $\overline{v}\langle T\rangle.P$ is ready to output message T on channel v, then to run P. In both of these, we may omit P when it is $\mathbf{0}$. When $(P_i)_{i\in I}$ is a finite set of of processes indexed by $I = 1..m$, we write $\prod_{i\in I} P_i$ as an abbreviation for $P_1 \mid \ldots \mid P_m$ (with $\prod_{i\in\varnothing} P_i = \mathbf{0}$).

Further, we extend processes with *active substitutions*:

Grammar for Extended Processes:

$A, B, C, I, K, S ::=$	extended processes
P	plain process
$A \mid B$	parallel composition
$\nu n.A$	name restriction
$\nu s.A$	variable restriction
$\{x = T\}$	active substitution

We write $\{x = T\}$ for the substitution that replaces the variable x with the term T. The substitution $\{x = T\}$ typically appears when the term T has been sent to the environment, but the environment may not have the atomic names that appear in T; the variable x is just a way to refer to T in this situation. The substitution $\{x = T\}$ is active in the sense that it "floats" and applies to any process that comes into contact with it. In order to control this contact, we may add a variable restriction: $\nu x.(\{x = T\} \mid P)$ corresponds exactly to *let* $x = T$ *in* P. Although the substitution $\{x = T\}$ concerns only one variable, we can build bigger substitutions by parallel composition. We always assume that our substitutions are cycle-free. We also assume that, in an extended process, there is at most one substitution for each variable, and there is exactly one when the variable is restricted.

A *frame* is an extended process built up from active substitutions by parallel composition and restriction. Informally, frames represent the static knowledge gathered by the environment after communications with an extended process. An *evaluation context* $E[\text{-}]$ is an extended process with a hole in the place of an extended process. As usual, names and variables have scopes, which are delimited by restrictions and by inputs. When X is any expression, $\mathit{fv}(X)$ and $\mathit{fn}(X)$ are the sets of free variables and free names of X, respectively.

We rely on a sort system for terms and extended processes [1, Section 2]. We always assume that terms and extended processes are well-sorted and that substitutions and context applications preserve sorts.

Given a signature Σ, we equip it with an equational theory (that is, with an equivalence relation on terms with certain closure properties). We write simply

$U = V$ to mean the terms U and V are related by the equational theory associated with Σ.

Structural equivalences, written $A \equiv B$, relate extended processes that are equal by any capture-avoiding rearrangements of parallel compositions, restrictions, and active substitutions, and by equational rewriting of any terms in processes.

Reductions, written $A \rightarrow B$, represent steps of computation (in particular, internal message transmissions and branching on conditionals). Reductions are closed by structural equivalence, hence by equational rewriting on terms.

Observational equivalences, written $A \approx B$, relate extended processes that cannot be distinguished by any evaluation context in the applied pi calculus, with any combination of messaging and term comparisons. (We let $\approx$ be the largest weak bisimulation on extended processes for reductions that preserves all potential observation of input or output on free names and that is closed by application of evaluation contexts [1].) *Strong equivalence*, written $A \sim B$, is a finer, auxiliary equivalence similarly defined by considering strong bisimulation and immediate observations. The applied pi calculus has a useful, general theory of observational equivalence, parameterized by Σ and its equational theory [1].

B Additional Proofs

We gather here proofs and additional lemmas that deal with internal choices, formula implementations, and logical equivalence in applied pi. These developments are not specific to the protocols considered in the paper.

B.1 Properties of Internal Choice

We begin by elaborating the co-inductive definition of internal choice given in the body of the paper. Let a binary relation $\mathcal{S}$ between processes and sets of processes be a *choice-relation* if and only if $P \mathrel{\mathcal{S}} X$ implies (1) if $Q \in X$ then $P \rightarrow^* \sim Q$; (2) if $P \rightarrow P'$, then either (a) $P' \sim Q$ for some $Q \in X$ or (b) $P' \mathrel{\mathcal{S}} X'$ for some $X' \subseteq X$; and (3) P does not communicate on free channel names.

Let $\mathcal{S}_\oplus$ be the union of all choice-relations. In effect, Section 4.1 takes $\bigoplus X$ to be the greatest choice-relation. By standard, simple arguments, the union of all choice-relations is in fact the greatest choice-relation. Hence, we have that $P \in \bigoplus X$ if and only if $P \mathrel{\mathcal{S}_\oplus} X$.

Next, we present some useful lemmas concerning internal choice.

Lemma 17 *If $P \sim Q$ and $Q \in \bigoplus X$ then $P \in \bigoplus X$.*

Proof This follows easily by definition of bisimilarity, $\sim$, and internal choice. $\square$

In our implementations, it is convenient to identify reduction steps that are deterministic, such as term comparisons; we introduce the relation $\rightarrow_d$ for these reduction steps. For the next lemma, we only need to assume that $\rightarrow$ and $\rightarrow_d$ commute, that is, $P \rightarrow_d Q$ and $P \rightarrow P'$ implies either $P' = Q$ or the existence of Q' with $P' \rightarrow_d Q'$ and $Q \rightarrow Q'$.

Lemma 18 *If $P \rightarrow_d Q$ and $Q \in \bigoplus X$ then $P \in \bigoplus X$.*

Proof This follows easily by definition of $P \rightarrow_d Q$ and internal choice. $\square$

Lemma 19 *If $P_i \in \bigoplus X_i$ for all $i \in I$ then $\bigoplus\{P_i \mid i \in I\} \subseteq \bigoplus \bigcup\{X_i \mid i \in I\}$.*

Proof Assume $P_i \in \bigoplus X_i$ for all $i \in I$.

Let $P \; \mathcal{S} \; X$ just if $P \in \bigoplus\{P_j \mid j \in J\}$ and $X = \bigcup\{X_j \mid j \in J\}$ for some $J \subseteq I$.

The lemma follows if the relation $\mathcal{S} \cup \mathcal{S}_\oplus$ is a choice-relation, for then we have that $\mathcal{S} \subseteq \mathcal{S}_\oplus$, and therefore that $P \; \mathcal{S}_\oplus \; \bigcup\{X_i \mid i \in I\}$ for all $P \in \bigoplus\{P_i \mid i \in I\}$, that is, $\bigoplus\{P_i \mid i \in I\} \subseteq \bigoplus \bigcup\{X_i \mid i \in I\}$.

To see that $\mathcal{S} \cup \mathcal{S}_\oplus$ is a choice-relation it suffices to consider any $P \in \bigoplus\{P_j \mid j \in J\}$ and $X = \bigcup\{X_j \mid j \in J\}$ for some $J \subseteq I$, and to establish the three conditions in the definition of a choice-relation.

(1) Consider any $Q \in X$ so that $Q \in X_j$ for some $j \in J$. By assumption, $P_j \in \bigoplus X_j$, and therefore $P_j \rightarrow^* \sim Q$. Since $P \in \bigoplus\{P_j \mid j \in J\}$, we have $P \rightarrow^* \sim P_j$, and therefore, by bisimilarity, $P \rightarrow^* \sim Q$.

(2) Suppose $P \rightarrow P'$. Since $P \in \bigoplus\{P_j \mid j \in J\}$, either (a) $P' \sim P_j$ for some $j \in J$ or (b) $P' \in \bigoplus\{P_j \mid j \in J'\}$ for some $J' \subseteq J$. In case (a), $P' \sim P_j \in \bigoplus X_j$ so $P' \in \bigoplus X_j$ by Lemma 17, and hence we have case (b), $P' \; \mathcal{S}_\oplus \; X_j$ with $X_j \subseteq X$. In case (b), we have case (b), $P' \; \mathcal{S} \; \bigcup\{X_j \mid j \in J'\} \subseteq X$ since $J' \subseteq J \subseteq I$.

(3) From $P \in \bigoplus\{P_j \mid j \in J\}$ it follows that P does not communicate on free channel names.

Hence, $\mathcal{S} \cup \mathcal{S}_\oplus$ is a choice-relation, and the lemma follows. $\square$

B.2 Properties of Formula Implementation

We state some basic facts concerning the implementation of a predicate Φ, with bound variables $\widetilde{y}$, as a process *filter* $\Phi \mapsto \widetilde{y}$ *in* P. The following may be proved by inductions on the definitions of the filters.

Lemma 20

(1) $\mathit{fv}(\mathit{filter}\ \Phi \mapsto \widetilde{y}\ \mathit{in}\ P) \subseteq (\mathit{fv}(\Phi) \cup \mathit{fv}(P)) \setminus \{\widetilde{y}\}$.

(2) $\mathit{fn}(\mathit{filter}\ \Phi \mapsto \widetilde{y}\ \mathit{in}\ P) \subseteq \mathit{fn}(\Phi) \cup \mathit{fn}(P)$.

(3) $(\mathit{filter}\ \Phi \mapsto \widetilde{y}\ \mathit{in}\ Q)\sigma = \mathit{filter}\ \Phi\sigma \mapsto \widetilde{y}\ \mathit{in}\ Q\sigma$ *when $\widetilde{y}$ do not occur in σ.*

Next, the main property of formula implementation to be proved here is Lemma 1.

Restatement of Lemma 1 *If filter $\Phi \mapsto \widetilde{y}$ in P is defined and closed then:*

$$\mathit{filter}\ \Phi \mapsto \widetilde{y}\ \mathit{in}\ P \quad \in \quad \bigoplus\{P\{\widetilde{y} = \widetilde{V}\} \mid \mathit{fv}(\widetilde{V}) = \varnothing \wedge \models \Phi\{\widetilde{y} = \widetilde{V}\}\}$$

Proof The proof is by induction on the definition of *filter* $\Phi \mapsto \widetilde{y}$ *in* P. Since *filter* $\Phi \mapsto \widetilde{y}$ *in* P is defined and closed, Lemma 20 implies we may assume that $fv(P) \subseteq \widetilde{y}$ and that $fv(\Phi) = \widetilde{y}$. We proceed by cases on the structure of Φ.

- In case $\Phi = (V = T)$, we are to show $Q \in \bigoplus X$, where

  $$\begin{array}{rcl} Q & = & \mathit{let}\ \widetilde{y} = \widetilde{S}\{x = V\}\ \mathit{in}\ \mathit{if}\ V = T\ \mathit{then}\ P \\ X & = & \bigoplus\{P\{\widetilde{y} = \widetilde{V}\} \mid fv(\widetilde{V}) = \varnothing \wedge (V = T)\{\widetilde{y} = \widetilde{V}\}\} \end{array}$$

  when $fv(T) = \widetilde{y}$, $fv(V) = \varnothing$, $fv(P) \subseteq \widetilde{y}$, and $V = T \mapsto \widetilde{y}$ with inverse terms $\widetilde{S}$.

  We consider two cases: either there are $\widetilde{V}$ such that $T\{\widetilde{y} = \widetilde{V}\} = V$, or not. In the first case, by clause (2) of the definition of $V = T \mapsto \widetilde{y}$, we have $\widetilde{V} = \widetilde{S}\{x = V\}$, and therefore the vector $\widetilde{V}$ is unique. We have:

  $$\begin{array}{rcl} Q & = & \mathit{if}\ V = T\{\widetilde{y} = \widetilde{S}\{x = V\}\}\ \mathit{then}\ P\{\widetilde{y} = \widetilde{S}\{x = V\}\} \\ & = & \mathit{if}\ V = T\{\widetilde{y} = \widetilde{V}\}\ \mathit{then}\ P\{\widetilde{y} = \widetilde{V}\} \\ & \rightarrow_d & P\{\widetilde{y} = \widetilde{V}\} \\ X & = & \{P\{\widetilde{y} = \widetilde{V}\} \mid fv(\widetilde{V}) = \varnothing \wedge T\{\widetilde{y} = \widetilde{V}\} = V\} \\ & = & \{P\{\widetilde{y} = \widetilde{V}\}\} \end{array}$$

  In the second case, when there are no $\widetilde{V}$ such that $T\{\widetilde{y} = \widetilde{V}\} = V$, we have:

  $$\begin{array}{rcl} Q & \rightarrow_d^* & \mathit{if}\ V = T\{\widetilde{y} = \widetilde{S}\{x = V\}\}\ \mathit{then}\ P\{\widetilde{y} = \widetilde{S}\{x = V\}\} \sim \mathbf{0} \\ X & = & \varnothing \end{array}$$

  Using Lemmas 17 and 18, we can establish $Q \in \bigoplus X$ in both cases.

- In case $\Phi = (x \in V)$ and $\widetilde{y} = \{x\}$, we are to show $Q \in \bigoplus X$ where

  $$\begin{array}{rcl} Q & = & \mathit{filter}\ x \in V \mapsto x\ \mathit{in}\ P \\ X & = & \{P\{x = U\} \mid (V = U_1\ \ldots\ U_i\, U\, V') \text{ for some } U_1, \ldots, U_i, U, V', i \geq 0\} \end{array}$$

  when $fv(V) = \varnothing$ and $fv(P) \subseteq \{x\}$. Now, by appeal to Lemma 6, the normal form of the closed term V must take the form $V = V_1 \ldots V_m\, W$ where $m \geq 0$ and $V_1, \ldots, V_m, W$ are closed, normal terms, and $W \neq W_1\, W_2$ for any W_1, W_2. We calculate as follows, where $R = s(z).\mathit{filter}\ z = h\ t \mapsto h, t\ \mathit{in}\ (\overline{c}\langle h\rangle \mid \overline{s}\langle t\rangle)$.

  $$\begin{array}{rcl} Q & = & \mathit{filter}\ x \in V_1 \cdots V_m\ W \mapsto x\ \mathit{in}\ P \\ & = & \nu s, c.(c(x).P \mid \overline{s}\langle V_1 \cdots V_m\ W\rangle \mid !R) \\ & \rightarrow_d^{2n} & \nu s, c.(c(x).P \mid \overline{c}\langle V_1\rangle \mid \ldots \mid \overline{c}\langle V_m\rangle \mid \overline{s}\langle W\rangle \mid !R) \\ & \rightarrow_d^2\sim & \nu c.(c(x).P \mid \overline{c}\langle V_1\rangle \mid \ldots \mid \overline{c}\langle V_m\rangle) \\ & \in & \bigoplus\{P\{x = V_i\} \mid i \in 1..m\} \\ & = & \bigoplus X \end{array}$$

  By Lemmas 17 and 18, $Q \in \bigoplus X$ follows.

- In case $\Phi = p(\widetilde{W})$, we are to show $Q \in \bigoplus \bigcup \{X_i \mid i \in 1..m\}$ where

$$\begin{array}{rcl} Q & = & \nu s.(\overline{s}\langle\epsilon\rangle \mid \prod_{i\in 1..m} s(\_).\mathit{filter}\ \Phi_i\{\widetilde{x} = \widetilde{W}\} \mapsto \widetilde{y}, \widetilde{z}_i\ \mathit{in}\ P) \\ X_i & = & \{P\{\widetilde{y} = \widetilde{V}\} \mid \mathit{fv}(\widetilde{U}, \widetilde{V}) = \varnothing \wedge \models \Phi_i\{\widetilde{x} = \widetilde{W}\}\{\widetilde{z}_i = \widetilde{U}\}\{\widetilde{y} = \widetilde{V}\}\} \end{array}$$

  when $\mathit{fv}(\widetilde{W}) = \widetilde{y}$, $\mathit{fv}(P) \subseteq \widetilde{y}$, and $p(\widetilde{x})$:- $\Phi_1 \vee \cdots \vee \Phi_m$ and, for all $i \in 1..m$, $\mathit{fv}(\Phi_i) = \widetilde{x} \uplus \widetilde{z}_i$ and $(\mathit{fv}(\widetilde{W}) \cup \mathit{fv}(P)) \cap \widetilde{z}_i = \varnothing$. By examining the m possible transitions of Q, we clearly have $Q \in \bigoplus\{P_i \mid i \in 1..m\}$, where:

$$P_i \quad = \quad \mathit{filter}\ \Phi_i\{\widetilde{x} = \widetilde{W}\} \mapsto \widetilde{y}, \widetilde{z}_i\ \mathit{in}\ P$$

  By induction hypothesis, for each $i \in 1..m$, $P_i \in \bigoplus X_i$. Hence, $\bigoplus\{P_i \mid i \in 1..m\} \subseteq \bigoplus \bigcup \{X_i \mid i \in 1..m\}$, by Lemma 19, and hence $Q \in \bigoplus \bigcup \{X_i \mid i \in 1..m\}$.

- In case $\Phi = \Phi_1, \Phi_2$, we are to show $Q \in \bigoplus X$ where

$$\begin{array}{rcl} Q & = & \mathit{filter}\ \Phi_1 \mapsto \widetilde{y}_1\ \mathit{in}\ (\mathit{filter}\ \Phi_2 \mapsto \widetilde{y}_2\ \mathit{in}\ P) \\ X & = & \{P\{\widetilde{y}_1, \widetilde{y}_2 = \widetilde{V}_1, \widetilde{V}_2\} \mid \\ & & \quad \models \Phi_1\{\widetilde{y}_1 = \widetilde{V}_1\} \wedge \models \Phi_2\{\widetilde{y}_1, \widetilde{y}_2 = \widetilde{V}_1, \widetilde{V}_2\} \wedge \mathit{fv}(\widetilde{V}_1, \widetilde{V}_2) = \varnothing\} \end{array}$$

  when $\mathit{fv}(P) \subseteq \widetilde{y}$, $\mathit{fv}(\Phi_1, \Phi_2) = \widetilde{y}$, $\widetilde{y}_1 = \widetilde{y} \cap \mathit{fv}(\Phi_1)$, and $\widetilde{y}_2 = \widetilde{y} \setminus \mathit{fv}(\Phi_1)$, so that $\widetilde{y} = \widetilde{y}_1 \uplus \widetilde{y}_2$. By induction hypothesis, $Q \in \bigoplus\{P_{\widetilde{V}_1} \mid \widetilde{V}_1 \in I\}$ where:

$$\begin{array}{rcl} P_{\widetilde{V}_1} & = & \mathit{filter}\ \Phi_2\{\widetilde{y}_1 = \widetilde{V}_1\} \mapsto \widetilde{y}_2\ \mathit{in}\ (P\{\widetilde{y}_1 = \widetilde{V}_1\}) \\ I & = & \{\widetilde{V}_1 \mid \mathit{fv}(\widetilde{V}_1) = \varnothing \wedge \models \Phi_1\{\widetilde{y}_1 = \widetilde{V}_1\}\} \end{array}$$

  By induction hypothesis, $P_{\widetilde{V}_1} \in \bigoplus X_{\widetilde{V}_1}$, for each $\widetilde{V}_1 \in I$, where:

$$\begin{array}{rcl} X_{\widetilde{V}_1} & = & \{P\{\widetilde{y}_1, \widetilde{y}_2 = \widetilde{V}_1, \widetilde{V}_2\} \mid \widetilde{V}_2 \in J_{\widetilde{V}_1}\} \\ J_{\widetilde{V}_1} & = & \{\widetilde{V}_2 \mid \mathit{fv}(\widetilde{V}_2) = \varnothing \wedge \models \Phi_2\{\widetilde{y}_1, \widetilde{y}_2 = \widetilde{V}_1, \widetilde{V}_2\}\} \end{array}$$

  Hence, with Lemma 19, we have:

$$\begin{array}{rcl} Q & \in & \bigoplus\{P_{\widetilde{V}_1} \mid \widetilde{V}_1 \in I\} \\ & \subseteq & \bigoplus \bigcup \{X_{\widetilde{V}_1} \mid \widetilde{V}_1 \in I\} \\ & = & \bigoplus\{P\{\widetilde{y}_1, \widetilde{y}_2 = \widetilde{V}_1, \widetilde{V}_2\} \mid \widetilde{V}_1 \in I, \widetilde{V}_2 \in J_{\widetilde{V}_1}\} \\ & = & \bigoplus X \end{array}$$

This completes all the cases of the induction. □

B.3 Properties of Logical Equivalence

We extend our definition of occurrence from events to sets of events as follows: we write $A \triangleright L$ when $L = \{\overline{a}\langle V\rangle \mid A \triangleright \overline{a}\langle V\rangle\}$. We can formulate robust safety (and other safety properties) using these observable sets: A is robustly safe if and only if, whenever $E[A] \rightarrow^* \triangleright L$, $E[\text{-}]$ does not bind the channels of L, and $\overline{end}\langle V\rangle \in L$, then also $\overline{begin}\langle V\rangle \in L$.

For a given set of processes X, the processes in $\bigoplus X$ are not necessarily observationally equivalent (as they may commit to different subsets of X). Still, we can substitute Q for P with $P, Q \in \bigoplus X$ without changing global set observations:

Lemma 21 *Internal choice implementations do not affect observations $A \rightarrow^* \triangleright L$.*

Proof In this proof, we say that two processes are *related* when they differ only on their implementation of internal choices: A and B are related when $A = F[\widetilde{S}]$, $B = F[\widetilde{S'}]$ for some m-ary context $F[\text{-}]$ and there exists X_i with $S_i, S'_i \in \bigoplus X_i$ for each $i \in 1..m$. (More general forms with nested internal choices are handled by transitivity.)

For any reduction step $A \rightarrow A'$, one of the following holds:

(1) $A \equiv E[S]$ for some X and $S \in \bigoplus X$, and

  (a) $A' \sim E[P]$ for some $P \in X$ (completion step); or

  (b) $A' \equiv E[S']$ for some $Y \subseteq X$ and $S' \in \bigoplus Y$ (internal step).

(2) $A \rightarrow A'$ does not depend on internal choice implementations (external step).

Internal and completion steps for different internal choices commute with one another, and internal steps commute with any external steps. Besides, condition (3) on internal choices implies that internal choices (and thus internal steps) never directly affect observations $A \triangleright L$.

Assume A and B are related. For any given L, we show that, if there exists A' such that $A \rightarrow^* A' \triangleright L$, then there exists B' such that $B \rightarrow^* B' \triangleright L$, by induction on the number of completion steps in $A \rightarrow^* A'$.

Base case (no completion step): by reordering reductions $A \rightarrow^* A'$, we obtain some A_1 with external steps $A \rightarrow^* A_1$ and internal steps $A_1 \rightarrow^* A'$. There exist external steps $B \rightarrow^* B_1$ in direct correspondence with $A \rightarrow^* A_1$ for some B_1 related to A_1. Finally, $A' \triangleright L$ implies $A_1 \triangleright L$, and we can conclude using $B \rightarrow^* B_1 \triangleright L$.

Inductive case: by reordering reductions $A \rightarrow^* A'$, we obtain

$$A \rightarrow^* \equiv E_A[S_A] \rightarrow^* \rightarrow E_A[P'] \rightarrow^* \equiv A'$$

where $E_A[\text{-}]$ is an evaluation context, X is a set of processes, and $S_A \in \bigoplus X$, $P \in X$, and $P' \sim P$ are processes with external steps $A \rightarrow^* E_A[S_A]$, internal steps and a first completion step $S_A \rightarrow^* \rightarrow P'$, and any steps $E_A[P'] \rightarrow^* \equiv A'$.

By definition of external step, we also have external steps $B \rightarrow^* E_B[S_B]$ such that $E_A[S_A]$ and $E_B[S_B]$ are related, for some $S_B \in \bigoplus X$ and evaluation context E_B[-].

By condition (1) on internal choice S_B, there exist $P'' \sim P$ with reductions $S_B \rightarrow^* P''$, and thus $E_B[S_B] \rightarrow^* E_B[P'']$ with $E_B[P''] \sim E_B[P']$. The processes $E_B[P']$ and $E_A[P']$ are related, hence, by induction hypothesis, $E_A[P'] \rightarrow^* A' \triangleright L$ implies $E_B[P'] \rightarrow^* \triangleright L$ and finally $B \rightarrow^* \triangleright L$. □

Next, we show that one can replace a formula by another (implementable) equivalent one without affecting set observations. This is useful to decompose message processing, as detailed in Section 4.4.

Lemma 22 *If A and B are logically equivalent and $A \rightarrow^* \triangleright L$, then also $B \rightarrow^* \triangleright L$.*

Proof This is Lemma 21 applied to the internal choices obtained by Lemma 1.□

Given the definition of robust safety, Lemma 3 now follows as a corollary.

Restatement of Lemma 3 *Logical equivalence preserves robust safety.*

C Namespaces

Element Namespaces:

Begin	*this paper*
Body	http://schemas.xmlsoap.org/soap/envelope/
CanonicalizationMethod	http://www.w3.org/2000/09/xmldsig#
Created	http://schemas.xmlsoap.org/ws/2002/07/utility
DigestMethod	http://www.w3.org/2000/09/xmldsig#
DigestValue	http://www.w3.org/2000/09/xmldsig#
End	*this paper*
Envelope	http://schemas.xmlsoap.org/soap/envelope/
Expires	http://schemas.xmlsoap.org/ws/2002/07/utility
Header	http://schemas.xmlsoap.org/soap/envelope/
KeyInfo	http://www.w3.org/2000/09/xmldsig#
Nonce	http://schemas.xmlsoap.org/ws/2002/07/secext
Password	http://schemas.xmlsoap.org/ws/2002/07/secext
Reference	http://www.w3.org/2000/09/xmldsig#
SecurityTokenReference	http://schemas.xmlsoap.org/ws/2002/07/secext
SignatureMethod	http://www.w3.org/2000/09/xmldsig#
SignatureValue	http://www.w3.org/2000/09/xmldsig#
SignedInfo	http://www.w3.org/2000/09/xmldsig#
Timestamp	http://schemas.xmlsoap.org/ws/2002/07/utility
Transforms	http://www.w3.org/2000/09/xmldsig#
Transform	http://www.w3.org/2000/09/xmldsig#
URI	http://www.w3.org/2000/09/xmldsig#
UsernameToken	http://schemas.xmlsoap.org/ws/2002/07/secext

Username	http://schemas.xmlsoap.org/ws/2002/07/secext
action	http://schemas.xmlsoap.org/rp
firewall	*this paper*
id	http://schemas.xmlsoap.org/rp
path	http://schemas.xmlsoap.org/rp
to	http://schemas.xmlsoap.org/rp

Attribute Namespaces:

Algorithm	http://www.w3.org/2000/09/xmldsig#
Id	http://schemas.xmlsoap.org/ws/2002/07/utility
mustUnderstand	http://schemas.xmlsoap.org/soap/envelope/
Type	http://schemas.xmlsoap.org/ws/2002/07/secext

D Sample Soap Messages

We include SOAP messages captured during actual runs of the protocols described in Sections 3.2, 3.3, and 3.4 using WSE 1.0 [29]. The first message shows the request and response messages for the unauthenticated web service; the second message illustrates username tokens with password digests; while the others illustrate signatures. We have indented the messages for clarity.

D.1 Unauthenticated Web Sevice

Request Message

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
               xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
               xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <soap:Header>
    <wsrp:path  soap:actor="http://schemas.xmlsoap.org/soap/actor/next"
                soap:mustUnderstand="1"
                xmlns:wsrp="http://schemas.xmlsoap.org/rp">
      <wsrp:action>http://msrc-688197/webservices/GetOrder</wsrp:action>
      <wsrp:to>http://localhost/MSPetshop/WebServices.asmx</wsrp:to>
      <wsrp:id>uuid:c2f12dbe-62dd-4bb5-ae39-6e94e41b27d6</wsrp:id>
    </wsrp:path>
    <wsu:Timestamp xmlns:wsu="http://schemas.xmlsoap.org/ws/2002/07/utility">
      <wsu:Created>2003-02-13T17:44:05Z</wsu:Created>
      <wsu:Expires>2003-02-13T17:49:05Z</wsu:Expires>
    </wsu:Timestamp>
  </soap:Header>
  <soap:Body>
    <GetOrder xmlns="http://msrc-688197/webservices/">
      <orderId>1</orderId>
    </GetOrder>
  </soap:Body>
</soap:Envelope>
```

Response Message

```
<soap:Envelope  xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
                xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <soap:Header>
    <wsu:Timestamp xmlns:wsu="http://schemas.xmlsoap.org/ws/2002/07/utility">
      <wsu:Created>2003-02-13T17:44:32Z</wsu:Created>
      <wsu:Expires>2003-02-13T17:49:32Z</wsu:Expires>
    </wsu:Timestamp>
  </soap:Header>
  <soap:Body>
    <GetOrderResponse xmlns="http://msrc-688197/webservices/">
      <GetOrderResult>
        <orderId>1</orderId>
        <date>2003-02-13T15:08:12.2330000-00:00</date>
        <userId>DotNet</userId>
        <cardType>Visa</cardType>
        <cardNumber>9999 9999 9999 9999</cardNumber>
        <cardExpiration>01/2002</cardExpiration>
        <billingAddress>
          <firstName>ABC</firstName>
          <lastName>XYX</lastName>
          <address1>901 San Antonio Road</address1>
          <address2>MS UCUP02-206</address2>
          <city>Palo Alto</city>
          <state>California</state>
          <zip>94303</zip>
          <country>USA</country>
        </billingAddress>
        <shippingAddress>
          <firstName>ABC</firstName>
          <lastName>XYX</lastName>
          <address1>901 San Antonio Road</address1>
          <address2>MS UCUP02-206</address2>
          <city>Palo Alto</city>
          <state>California</state>
          <zip>94303</zip>
          <country>USA</country>
        </shippingAddress>
        <lineItems>
          <item>
            <id>EST-2     </id>
            <line>1</line>
            <quantity>1</quantity>
            <price>16.5</price>
          </item>
        </lineItems>
      </GetOrderResult>
    </GetOrderResponse>
  </soap:Body>
</soap:Envelope>
```

D.2 Password Digest

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
               xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
               xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <soap:Header>
    <wsse:Security
          soap:mustUnderstand="1"
          xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/07/secext">
      <wsse:UsernameToken
            xmlns:wsu="http://schemas.xmlsoap.org/ws/2002/07/utility"
            wsu:Id="SecurityToken-8d8ad486-4db2-41b3-a78b-35985b1e83bf">
        <wsse:Username>DotNet</wsse:Username>
        <wsse:Password
              Type="wsse:PasswordDigest"
               >sp7MxkRDIW7vda0/5abw40wzByM=</wsse:Password>
        <wsse:Nonce>5yRhP7n9f53yvis5B9m4cA==</wsse:Nonce>
        <wsu:Created>2003-04-16T15:40:13Z</wsu:Created>
      </wsse:UsernameToken>
    </wsse:Security>
  </soap:Header>
  <soap:Body>
    <GetOrder xmlns="http://tempuri.org/">
      <orderId>1</orderId>
    </GetOrder>
  </soap:Body>
</soap:Envelope>
```

D.3 Password-based Signature

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
               xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
               xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <soap:Header>
    <wsse:Security
          soap:mustUnderstand="1"
          xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/07/secext">
      <wsse:UsernameToken
            xmlns:wsu="http://schemas.xmlsoap.org/ws/2002/07/utility"
            wsu:Id="SecurityToken-5942b215-fe80-4e6c-9547-c3ee5023974a">
        <wsse:Username>DotNet</wsse:Username>
        <wsse:Password
              Type="wsse:PasswordDigest"
```

```
               >1OhGjpImnOkwH2bP5wgPsO535Cg=</wsse:Password>
        <wsse:Nonce>/MN387Y8ZQEhbkUeERqmEA==</wsse:Nonce>
        <wsu:Created>2003-04-16T15:40:46Z</wsu:Created>
      </wsse:UsernameToken>
      <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
        <SignedInfo>
          <CanonicalizationMethod
               Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
          <SignatureMethod
               Algorithm="http://www.w3.org/2000/09/xmldsig#hmac-sha1" />
          <Reference URI="#Id-40db2c1e-781c-4dba-b4ba-ab933989c275">
            <Transforms>
              <Transform
                   Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </Transforms>
            <DigestMethod
                 Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
            <DigestValue>WHaqWVi124JJzfDOIOWJOFLodcI=</DigestValue>
          </Reference>
        </SignedInfo>
        <SignatureValue>fzVrKRrsLTfSyLdW4a3TP5w8SiE=</SignatureValue>
        <KeyInfo>
          <wsse:SecurityTokenReference>
            <wsse:Reference
               URI="#SecurityToken-5942b215-fe80-4e6c-9547-c3ee5023974a" />
          </wsse:SecurityTokenReference>
        </KeyInfo>
      </Signature>
    </wsse:Security>
  </soap:Header>
  <soap:Body wsu:Id="Id-40db2c1e-781c-4dba-b4ba-ab933989c275"
             xmlns:wsu="http://schemas.xmlsoap.org/ws/2002/07/utility">
    <GetOrder xmlns="http://tempuri.org/">
      <orderId>1</orderId>
    </GetOrder>
  </soap:Body>
</soap:Envelope>
```

D.4 X.509 Signature

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
               xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
               xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <soap:Header>
    <wsrp:path soap:actor="http://schemas.xmlsoap.org/soap/actor/next"
               soap:mustUnderstand="1"
               xmlns:wsrp="http://schemas.xmlsoap.org/rp">
      <wsrp:action wsu:Id="Id-0b823d56-6677-49a5-b414-c7b3e60599f8"
                   xmlns:wsu="http://schemas.xmlsoap.org/ws/2002/07/utility"
              >http://msrc-688197/webservices/GetOrder</wsrp:action>
      <wsrp:to wsu:Id="Id-19f43ec9-fc7d-4c70-82df-3f008731fa44"
               xmlns:wsu="http://schemas.xmlsoap.org/ws/2002/07/utility"
              >http://localhost/MSPetshop/WebServices.asmx</wsrp:to>
      <wsrp:id wsu:Id="Id-33af1237-0a2b-467f-b30c-9ed92d5ec678"
               xmlns:wsu="http://schemas.xmlsoap.org/ws/2002/07/utility"
              >uuid:4e459eec-841c-4c86-9f21-67228c4165b2</wsrp:id>
    </wsrp:path>
    <wsse:Security soap:mustUnderstand="1"
                   xmlns:wsse="http://schemas.xmlsoap.org/ws/2002/07/secext">
      <wsse:BinarySecurityToken
            ValueType="wsse:X509v3"
            EncodingType="wsse:Base64Binary"
            xmlns:wsu="http://schemas.xmlsoap.org/ws/2002/07/utility"
            wsu:Id="SecurityToken-323b80ff-5a7e-4df4-ab71-918ade86decd"
           >MIIHTjCCBjagAwIBAgIKbCnd3gAAAAiNNjANBg...</wsse:BinarySecurityToken>
      <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
        <SignedInfo>
          <CanonicalizationMethod
              Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
          <SignatureMethod
              Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
          <Reference URI="#Id-bcf3bbe8-fd96-4483-97d3-2dfb220bd8b1">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
            <DigestValue>vwMT/J77QuAehktMqF+FiOuuyvc=</DigestValue>
          </Reference>
          <Reference URI="#Id-0b823d56-6677-49a5-b414-c7b3e60599f8">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
            <DigestValue>vl9nyklaH25kKH4cRNYsrb0Ygg4=</DigestValue>
          </Reference>
          <Reference URI="#Id-19f43ec9-fc7d-4c70-82df-3f008731fa44">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
            <DigestValue>JI+t02Q3FPDzWaizhiFV1EDU9H8=</DigestValue>
          </Reference>
          <Reference URI="#Id-33af1237-0a2b-467f-b30c-9ed92d5ec678">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
            <DigestValue>bzImlmlAjr55yh3YceedFbwY8S4=</DigestValue>
          </Reference>
        </SignedInfo>
```

```
        <SignatureValue>tW1VsomxSeaVCLQ5xCwjRLxA73...=</SignatureValue>
        <KeyInfo>
          <wsse:SecurityTokenReference>
            <wsse:Reference
                  URI="#SecurityToken-323b80ff-5a7e-4df4-ab71-918ade86decd" />
          </wsse:SecurityTokenReference>
        </KeyInfo>
      </Signature>
    </wsse:Security>
  </soap:Header>
  <soap:Body wsu:Id="Id-bcf3bbe8-fd96-4483-97d3-2dfb220bd8b1"
           xmlns:wsu="http://schemas.xmlsoap.org/ws/2002/07/utility">
    <GetOrder xmlns="http://msrc-688197/webservices/">
      <orderId>1</orderId>
    </GetOrder>
  </soap:Body>
</soap:Envelope>
```

References

[1] M. Abadi and C. Fournet. Mobile values, new names, and secure communication. In *28th ACM Symposium on Principles of Programming Languages (POPL'01)*, pages 104–115, 2001.

[2] M. Abadi, C. Fournet, and G. Gonthier. Authentication primitives and their compilation. In *27th ACM Symposium on Principles of Programming Languages (POPL'00)*, pages 302–315, 2000.

[3] B. Atkinson, G. Della-Libera, S. Hada, M. Hondo, P. Hallam-Baker, C. Kaler, J. Klein, B. LaMacchia, P. Leach, J. Manferdelli, H. Maruyama, A. Nadalin, N. Nagaratnam, H. Prafullchandra, J. Shewchuk, and D. Simon. Web services security (WS-Security), version 1.0. At `http://msdn.microsoft.com/library/en-us/dnglobspec/html/ws-security.asp`. Draft submitted to OASIS Web Services Security TC, April 2002.

[4] F. Baader and T. Nipkow. *Term Rewriting and All That*. Cambridge University Press, 1998.

[5] K. Bhargavan, C. Fournet, and A. D. Gordon. A semantics for web services authentication. In *31st ACM Symposium on Principles of Programming Languages (POPL'04)*, pages 198–209, 2004.

[6] B. Blanchet. From secrecy to authenticity in security protocols. In *Proceedings of the 9th International Static Analysis Symposium (SAS'02)*, volume 2477 of *LNCS*, pages 342–359. Springer, 2002.

[7] D. Box, D. Ehnebuske, G. Kakivaya, A. Layman, N. Mendelsohn, H. Nielsen, S. Thatte, and D. Winer. *Simple Object Access Protocol (SOAP) 1.1*, 2000. W3C Note, at `http://www.w3.org/TR/2000/NOTE-SOAP-20000508/`.

[8] J. Boyer. *Canonical XML*, 2001. W3C Recommendation, at http://www.w3.org/TR/2001/REC-xml-c14n-20010315/.

[9] J. Boyer, D. E. Eastlake, and J. Reagle. *Exclusive XML Canonicalization*, 2002. W3C Recommendation, at http://www.w3.org/TR/2002/REC-xml-exc-c14n-20020718/.

[10] M. Burrows, M. Abadi, and R. Needham. A logic of authentication. *Proceedings of the Royal Society of London A*, 426:233–271, 1989.

[11] E. Cohen. TAPS: A first-order verifier for cryptographic protocols. In *13th IEEE Computer Security Foundations Workshop*, pages 144–158. IEEE Computer Society Press, 2000.

[12] J. Cowan and R. Tobin. *XML Information Set*, 2001. W3C Recommendation, at http://www.w3.org/TR/2001/REC-xml-infoset-20011024/.

[13] E. Damiani, S. De Capitani di Vimercati, S. Paraboschi, and P. Samarati. Securing SOAP e-services. *International Journal of Information Security*, 1(2):100–115, 2002.

[14] E. Damiani, S. De Capitani di Vimercati, and P. Samarati. Towards securing XML web services. In *ACM Workshop on XML Security 2002*, pages 90–96, 2003.

[15] G. Della-Libera, P. Hallam-Baker, M. Hondo, C. K. (Editor), H. Maruyama, A. Nadalin, N. Nagaratnam, H. Prafullchandra, J. Shewchuk, K. Tamura, and H. Wilson. Web services security addendum version 1.0. At http://msdn.microsoft.com/library/en-us/dnglobspec/html/ws-security-addendum.asp, August 2002.

[16] T. Dierks and C. Allen. The TLS protocol: Version 1.0, 1999. RFC 2246.

[17] D. Dolev and A. Yao. On the security of public key protocols. *IEEE Transactions on Information Theory*, IT–29(2):198–208, 1983.

[18] D. Eastlake and P. Jones. US Secure Hash Algorithm 1 (SHA1), 2001. RFC 3174.

[19] D. Eastlake, J. Reagle, D. Solo, M. Bartel, J. Boyer, B. Fox, B. LaMacchia, and E. Simon. *XML-Signature Syntax and Processing*, 2002. W3C Recommendation, at http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/.

[20] C. Fournet and M. Abadi. Hiding names: Private authentication in the applied pi calculus. In M. Okada, B. Pierce, A. Scedrov, H. Tokuda, and A. Yonezawa, editors, *Software Security – Theories and Systems. Mext-NSF-JSPS International Symposium, Tokyo, Nov. 2002 (ISSS'02)*, volume 2609 of *LNCS*, pages 317–338. Springer, 2003.

[21] A. D. Gordon and A. Jeffrey. Authenticity by typing for security protocols. *Journal of Computer Security*, 11(4):451–521, 2003.

[22] A. D. Gordon and R. Pucella. Validating a web service security abstraction by typing. In *ACM Workshop on XML Security 2002*, pages 18–29, 2003.

[23] J. Jonsson and B. Kaliski. Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, 2003. RFC 3447.

[24] R. Kemmerer, C. Meadows, and J. Millen. Three systems for cryptographic protocol analysis. *Journal of Cryptology*, 7(2):79–130, 1994.

[25] H. Krawczyk, M. Bellare, and R. Canetti. HMAC: Keyed-hashing for message authentication, 1997. RFC 2104.

[26] G. Lowe. Breaking and fixing the Needham-Schroeder public-key protocol using CSP and FDR. In *Tools and Algorithms for the Construction and Analysis of Systems*, volume 1055 of *LNCS*, pages 147–166. Springer, 1996.

[27] G. Lowe. A hierarchy of authentication specifications. In *Proceedings of 10th IEEE Computer Security Foundations Workshop, 1997*, pages 31–44. IEEE Computer Society Press, 1997.

[28] Microsoft Corporation. *Microsoft .NET Pet Shop*, 2002. At `http://www.gotdotnet.com/team/compare/petshop.aspx`.

[29] Microsoft Corporation. *Web Services Enhancements for Microsoft .NET*, Dec. 2002. At `http://msdn.microsoft.com/webservices/building/wse/default.aspx`.

[30] R. Milner. *Communicating and Mobile Systems: the π-Calculus.* Cambridge University Press, 1999.

[31] A. Nadalin, C. Kaler, P. Hallam-Baker, and R. Monzillo. *Web Services Security: SOAP Message Security*, Aug. 2003. At `http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss`.

[32] R. Needham and M. Schroeder. Using encryption for authentication in large networks of computers. *Commun. ACM*, 21(12):993–999, 1978.

[33] H. F. Nielsen and S. Thatte. Web services routing protocol (WS-Routing). At `http://msdn.microsoft.com/library/en-us/dnglobspec/html/ws-routing.asp`, October 2001.

[34] L. Paulson. The inductive approach to verifying cryptographic protocols. *Journal of Computer Security*, 6:85–128, 1998.

[35] J. H. Saltzer, D. P. Reed, and D. D. Clark. End-to-end arguments in system design. *ACM Transactions in Computer Systems*, 2(4):277–288, November 1984.

[36] M. Satyanarayanan. Integrating security in a large distributed system. *ACM Trans. Comput. Syst.*, 7(3):247–280, 1989.

[37] J. Siméon and P. Wadler. The essence of XML. In *30th ACM Symposium on Principles of Programming Languages (POPL'03)*, pages 1–13, 2003.

[38] F. Thayer Fábrega, J. Herzog, and J. Guttman. Strand spaces: Proving security protocols correct. *Journal of Computer Security*, 7:191–230, 1999.

[39] L. van Doorn, M. Abadi, M. Burrows, and E. Wobber. Secure network objects. In *IEEE Computer Society Symposium on Research in Security and Privacy*, pages 211–221, 1996.

[40] W. Vogels. Web services are not distributed objects. *IEEE Internet Computing*, 7(6):59–66, 2003.

[41] T. Woo and S. Lam. A semantic model for authentication protocols. In *IEEE Computer Society Symposium on Research in Security and Privacy*, pages 178–194, 1993.