A Preparation

Our formal security analysis of UPPRESSO is based on the general Dolev-Yao web model in SPRESSO. To facilitate the definition of UPPRESSO, however, we have some difference from SPRESSO. In particular, we remove some processes and add some function symbols for asymmetric encryption/decryption.

A.1 Functions Symbols

Since our model is using ECC(Elliptic Curve Cryptography) to encrypt/decrypt the data, we add the following symbols to the signature Σ for the terms and messages:

- $\mathbb{E}$ is an elliptic curve over a finite field $\mathbb{F}_q$, G is a base point(or generator) of $\mathbb{E}$ and the order of G is a prime number n.
- $[t]P$ means using asymmetric key t to encrypt the point $P = [p]G$ on the elliptic curve where p is the actual plaintext.
- $[t^{-1}]C$ means using the reverse of t to decrypt the point $C = [c]G = [tm]G$ on the elliptic curve where c is the cipertext.
- $\texttt{isValid}(P)$ checks whether P is a valid point on the elliptic curve. That is to say whether $P = [m]G$ for the base point G and some nonce m.

A.2 DNS servers

In SPRESSO, when receiving an e-mail address, RP needs to send DNS requests to DNS servers manually to fetch the information of the IdP server. Since there may be various DNS servers in SPRESSO, DNS server security issues need to be given special consideration. As a result, DNS servers are added into the formal model of SPRESSO.

In UPPRESSO, however, we only have one centralized IdP server, and all RPs know the relevant information of the IdP in advance. So all DNS requests are generated spontaneously by the browser, not introduced by our scripts. Therefore, we remove DNS servers from the formal model of UPPRESSO.

B Formal Model of UPPRESSO

We here present the full details of our formal model of UPPRESSO. For our analysis regarding our authentication and privacy properties below, we will further restrict this generic model to suit the setting of respective analysis.

We model UPPRESSO as a web system. We call a web system $\mathcal{UWS} = (\mathcal{W}, \mathcal{S}, \mathsf{script}, E^0)$ an UPPRESSO web system if it is of the form described in what follows.

B.1 Outline

The system $\mathcal{W} = \mathsf{Hon} \cup \mathsf{Web} \cup \mathsf{Net}$ consists of web attacker processes (in Web), network attacker processes (in Net), a finite set B of web browsers, a finite set RP of web servers for the relying parties, a finite set IDP of web servers containing only one identity provider with $\mathsf{Hon} := \mathsf{B} \cup \mathsf{RP} \cup \mathsf{IDP}$. More details on the processes in $\mathcal{W}$ are provided below. Figure 1 shows the set of scripts $\mathcal{S}$ and their respectice string representations that are defined by the mapping script. The set E^0 contains only the trigger events.

$s \in \mathcal{S}$	$\mathsf{script}(s)$
R^{att}	`att_script`
$\mathit{script\_rp}$	`script_rp`
$\mathit{script\_idp}$	`script_idp`

Figure 1: List of scripts in $\mathcal{S}$ and their respective string representations.

This outlines $\mathcal{UWS}$. We will define the DY processes in $\mathcal{UWS}$ and their addresses, domain names, and secrets in more detail. The scripts are defined in detail in Appendix B.14

B.2 Addresses and Domain Names

The set IPs contains for every web attacker in Web, every network attacker in Net, every relying party in RP, the only one identity provider in IDP, and every browser in B a finite set of addresses each. By addr we denote the corresponding assignment from a process to its address. The set Doms contains a finite set of domains for every relying party in RP, the only one identity provider in IDP, every web attacker in Web, and every network attacker in Net. Browsers (in B) do not have a domain.

By addr and dom we denote the assignments from atomic processes to sets of IPs and Doms, respectively.

B.3 Keys and Secrets

The set $\mathcal{N}$ of nonces is partitioned into four sets, an infinite sequence N, an infinite set K_{SSL}, an infinite set K_{sign}, an infinite set K_{id}, an infinite set K_{point}, and a finite set Secrets. We thus have

$$\mathcal{N} = \underbrace{N}_{\text{infinite sequence}} \dot\cup \underbrace{K_{\text{SSL}}}_{\text{finite}} \dot\cup \underbrace{K_{\text{sign}}}_{\text{finite}} \dot\cup \underbrace{K_{\text{point}}}_{\text{finite}} \dot\cup \underbrace{\mathsf{Secrets}}_{\text{finite}} .$$

The set N contains the nonces that are available for each DY process in $\mathcal{W}$ (it can be used to create a run of $\mathcal{W}$).

The set K_{SSL} contains the keys that will be used for SSL encryption. Let $\mathsf{tlskey}\colon \mathsf{Doms} \to K_{\text{SSL}}$ be an injective mapping that assigns a (different) private key to every domain.

The set K_{sign} contains the keys that will be used by IdPs for signing IAs. Let $\mathsf{signkey}\colon \mathsf{IdPs} \to K_{\text{sign}}$ be an injective mapping that assigns a (different) private key to every identity provider.

The set K_{point} contains all valid points on the curve. The set K_{point} will be used to generate identities of B and RP.

The set $\mathsf{Secrets}$ is the set of passwords (secrets) the browsers share with the identity providers.

B.4 Identities

There are many different types of identities in UPPRESSO, We denote the identity of the broswer at the IdP with u, the identity of the relying party at the IdP with r and the identity of the broswer at the relying party with $acct$. The details are defined below.

Definition 1. *An* identity u *is a term of the form* $u = \langle id, username, domain_{idp}\rangle$ *with* $id \in N$*,* $username \in \mathbb{S}$ *and* $domain_{idp} \in \mathsf{Doms}$*.*

Definition 2. *An* identity r *is a term of the form* $r = \langle id, commonname, domain_{idp}\rangle$ *with* $id \in K_{point}$*,* $commonname \in \mathbb{S}$ *and* $domain_{idp} \in \mathsf{Doms}$*.*

Definition 3. *An* identity $acct$ *is a term of the form* $acct = \langle\langle acct_1, domain_{rp_1}\rangle, \langle acct_2, domain_{rp_2}\rangle, \ldots\rangle$ *.* *with* $acct_i \in K_{point}$*,* $domain_{rp_i} \in \mathsf{Doms}$*.*

Let ID^u be the finite set of identities u.

By $\mathsf{secretOfID} : \mathsf{ID}^u \to \mathsf{Secrets}$ we denote the bijective mapping that assigns secrets to all identities.

Let $\mathsf{ownerOfSecret} : \mathsf{Secrets} \to \mathsf{B}$ denote the mapping that assigns to each secret a browser that *owns* this secret. Now, we define the mapping $\mathsf{ownerOfID} : \mathsf{ID}^u \to \mathsf{B}$, $i \mapsto \mathsf{ownerOfSecret}(\mathsf{secretOfID}(i))$, which assigns to each identity the browser that owns this identity (we say that the identity belongs to the browser).

To be concise, we usually use u and r to refer to $u.id$ and $r.id$ if we don't say they are identities or $u, r \in \mathsf{ID}$

B.5 Tags, Identity Tokens and Service Tokens

Definition 4. *A* tag *is a term of the form* $PID_{rp} = [t]ID_{rp} = [tr]G$ *for a nonce (here used as a asymmetric key)* t*.*

Definition 5. *An* identity Tokens (IDToken) *is a term of the form* $\langle PID_{rp}, PID_u, ver\rangle$ *for a tag* PID_{rp}*, an encrypted identity* $PID_u = [u]PID_{rp} = [utr]G$ *and a signature* $ver = \mathsf{sig}(\langle PID_{rp}, PID_u\rangle, k)$ *for a nonce* k*.*

Definition 6. *A* service token *is a term of the form* $\langle nonce, Acct\rangle$ *with* $Acct = [t^{-1}]PID_u = [t^{-1}][utr]G = [ur]G$ *for a nonce* t*.*

B.6 Corruption

RPs can become corrupted: If they receive the message `CORRUPT`, they start collecting all incoming messages in their state and (upon triggering) send out all messages that are derivable from their state and collected input messages, just like the attacker process. We say that an RP is *honest* if the according part of their state ($s.\mathtt{corrupt}$) is $\perp$, and that they are corrupted otherwise.

We are now ready to define the processes in $\mathcal{W}$ as well as the scripts in $\mathcal{S}$ in more detail.

B.7 Processes in $\mathcal{W}$ (Overview)

We first provide an overview of the processes in $\mathcal{W}$. All processes in $\mathcal{W}$ contain in their initial states all public keys and the private keys of their respective domains (if any). We define $I^p = \mathsf{addr}(p)$ for all $p \in \mathsf{Hon} \cup \mathsf{Web}$.

Web Attackers. Each $wa \in \mathsf{Web}$ is a web attacker who uses only his own addresses for sending and listening.

Network Attackers. Each $na \in \mathsf{Net}$ is a network attacker who uses all addresses for sending and listening.

Browsers. Each $b \in \mathsf{B}$ is a web browser. The initial state contains all secrets owned by b, stored under the origin of the respective IdP. See Appendix B.11 for details.

Relying Parties. A relying party $r \in \mathsf{RP}$ is a web server. RP knows four distinct paths: `/script`, where it serves `script_rp` to open a new window and facilitate the login flow. `/loginSSO`, where it only accepts GET requests and sends redirect response to redirect the browser to the IdP to download `script_IdP` `/startNegotiation`, where it only accepts POST requests logically sent from `script_rp` using postMessge and checks whether the data $t \in K_{\text{id}}$. If the request valid, it send back a certificate. `/uploadToken` running in the browser. It checks the ID token and, if the data is deemed "valid", it issues a service token (again, for details, see below). Intuitively, a client having such a token can use the service of the RP (for a specific identity record along with the token). Just like IdPs, RPs can become corrupted.

Identity Providers. Each IdP is a web server, users can authenticate to the IdP with their credentials. IdP tracks the state of the users with sessions. Authenticated users can receive IDTokens from the IdP.

B.8 TLS Key Mapping

Before we define the atomic DY processes in more detail, we first define the common data structure that holds the mapping of domain names to public TLS keys: For an atomic DY process p we define

$$tlskeys^p = \langle \{ \langle d, \mathsf{tlskey}(d) \rangle \mid d \in \mathsf{dom}(p) \} \rangle.$$

B.9 Web Attackers

Each $wa \in \mathsf{Web}$ is a web attacker. The initial state of each wa is $s_0^{wa} = \langle \mathit{attdoms}, \mathit{tlskeys}, \mathit{signkeys} \rangle$, where $\mathit{attdoms}$ is a sequence of all domains along with the corresponding private keys owned by wa, $\mathit{tlskeys}$ is a sequence of all domains and the corresponding public keys, and $\mathit{signkeys}$ contains the public signing key for the IdP.

B.10 Network Attackers

As mentioned, each network attacker na is modeled to be a network attacker. We allow it to listen to/spoof all available IP addresses, and hence, define $I^{na} = \mathsf{IPs}$. The initial state is $s_0^{na} = \langle \mathit{attdoms}, \mathit{tlskeys}, \mathit{signkeys} \rangle$, where $\mathit{attdoms}$ is a sequence of all domains along with the corresponding private keys owned by the attacker na, $\mathit{tlskeys}$ is a sequence of all domains and the corresponding public keys, and $\mathit{signkeys}$ contains the public signing key for the IdP.

B.11 Browsers

Each $b \in \mathsf{B}$ is a web browser with $I^b := \mathsf{addr}(b)$ being its addresses.

To define the inital state, first let $ID^b := \mathsf{ownerOfID}^{-1}(b)$ be the set of all IDs of b, Then, the initial state s_0^b is defined as follows: the key mapping maps every domain to its public (ssl) key, according to the mapping tlskey; the DNS address is $\mathsf{addr}(p)$ with $p \in \mathcal{W}$; the list of secrets contains an entry $\langle \langle d, \mathsf{S} \rangle, s \rangle$ for each $d \in \mathit{SecretDomains}^b$ and $s = \mathsf{secretOfID}(i)$ for some $i \in ID^{b,d}$ (s is the same for all i); ids is $\langle ID^b \rangle$; sts is empty.

B.12 Relying Parties

A relying party $r \in \mathsf{RP}$ is a web server modeled as an atomic DY process (I^r, Z^r, R^r, s_0^r) with the addresses $I^r := \mathsf{addr}(r)$. Its initial state s_0^r contains its domains, the private keys associated with its domains. The full state additionally contains the sets of service tokens and login session identifiers the RP has issued. RP only accepts HTTPS requests.

RP manages two kinds of sessions: The *login sessions*, which are only used during the login phase of a user, and the *service sessions* (we call the session identifier of a service session a *service token*). Service sessions allow a user to use RP's services. The ultimate goal of a login flow is to establish such a service session.

In a typical flow with one client, r will first receive an HTTP GET request for the path `/script`. In this case, r returns the script `script_rp` (see below).

After the user loaded the script in his browser, r will receive an HTTP GET request for the path `/loginSSO` sent from the new window opened by `script_rp`. In this request, r will send back a redirect response for downloading `script_IdP` from IdP.

When the IdP document in the browser generates a number t, r will receive the third request for the path `/startNegotiate`. r will verify t and if valid,

r will create the corresponding login session with a *loginSessionToken* as the identifier. After that, r will use t to generate PID_{rp} and bind it with the login session. After all these are down, r send its certificate signed by the specific IdP that browser selected.

Finally, r receives a last request in the login flow. This POST request contains the IDToken. To conclude the login, r looks up the user's login session, compare the $\mathit{IDToken}.\mathtt{PID_{rp}}$ with the PID_{rp} in the login session, and checks whether $\mathit{IDToken}.\mathtt{PID_{ver}}$ is a correct signature. If successful, r calculates the service token and returns it, which is also stored in the state of r.

If r receives a corrupt message, it becomes corrupt and acts like the attacker from then on.

We now provide the formal definition of r as an atomic DY process (I^r, Z^r, R^r, s_0^r). As mentioned, we define $I^r = \mathsf{addr}(r)$. Next, we define the set Z^r of states of r and the initial state s_0^r of r.

Definition 7. *A* login session record *is a term of the form* $\langle t, PID_{rp} \rangle$ *with* $t, PID_{rp} = [tr]G(t, r \in K_{id})$.

Definition 8. *A* state $s \in Z^r$ of an RP r *is a term of the form* $\langle \mathit{keyMapping},\ \mathit{tlskeys},\ \mathit{loginSessions},\ \mathit{serviceTokens},\ \mathit{corrupt},\ \mathit{IdPConfig},\ \mathit{rp} \rangle$ *where* $\mathit{keyMapping} \in [\mathbb{S} \times \mathcal{N}]$, $\mathit{tlskeys} = \mathit{tlskeys}^r$, $\mathit{serviceTokens} \in \mathcal{N}$, $\mathit{loginSessions} \in \left[\mathcal{N} \times \mathcal{T}_{\mathcal{N}}\right]$ *is a dictionary of login session records,* $\mathit{corrupt} \in \mathcal{T}_{\mathcal{N}}$, $\mathit{IdPConfig} \in \mathcal{T}_{\mathcal{N}}$ *is the configuration retrieved from IdP server,* $\mathit{rp} \in \mathsf{ID}$ *is the identity of the RP, see details in Appendix B.4.*

The initial state s_0^r of r *is a state of* r *with* $s_0^r.\mathtt{serviceTokens} = s_0^r.\mathtt{loginSessions} = \langle\rangle$, $s_0^r.\mathtt{corrupt} = \bot$, $s_0^r.\mathtt{keyMapping}$ *is the same as the keymapping for browsers above,* $s_0^r.\mathtt{IdPConfig} = \langle \mathit{pubkey}, \mathit{scriptUrl}, \mathit{Cert}_{rp} \rangle$ *and* $s_0^r.\mathtt{rp} = \langle \mathit{id}, \mathit{commonname}, \mathit{domain}_{idp} \rangle$.

We now specify the relation R^r. We describe this relation by a non-deterministic algorithm.

Algorithm 1 Relation of a Relying Party R^r

```
Input: $\langle a, b, m \rangle, s$
let $s' := s$
if $s'.\mathtt{corrupt} \not\equiv \bot \lor m \equiv \mathtt{CORRUPT}$ then
    let $s'.\mathtt{corrupt} := \langle \langle a, f, m \rangle, s'.\mathtt{corrupt} \rangle$
    let $m' := d_V(s')$
    let $a' := \mathsf{IPs}$
    stop $\langle a', a, m' \rangle, s'$
end if
let $m_{dec}, k, k', \mathit{inDomain}$ such that
    $\hookrightarrow$ $\langle m_{\mathrm{dec}}, k \rangle \equiv \mathsf{dec_a}(m, k') \land \langle \mathit{inDomain}, k' \rangle \in s'.\mathtt{sslkeys}$
    $\hookrightarrow$ if possible; otherwise stop $\langle\rangle, s'$
let $n, \mathit{method}, \mathit{path}, \mathit{parameters}, \mathit{headers}, \mathit{body}$ such that
    $\hookrightarrow$ $\langle \mathtt{HTTPReq}, n, \mathit{method}, \mathit{path}, \mathit{parameters}, \mathit{headers}, \mathit{body} \rangle \equiv m_{dec}$
    $\hookrightarrow$ if possible; otherwise stop $\langle\rangle, s'$
if $\mathit{path} \equiv /\mathit{script}$ then
```

```
    let $m' := \mathsf{enc_s}(\langle \mathtt{HTTPResp}, n, 200, \langle\rangle, \mathtt{script\_rp}\rangle, k)$
    stop $\langle b, a, m'\rangle, s'$
else if $path \equiv /loginSSO$ then
    let $m' := \mathsf{enc_s}(\langle \mathtt{HTTPResp}, n, 302, \langle\langle \mathtt{Location}, s'.\mathtt{IdPConfig}.scriptUrl\rangle\rangle, \langle\rangle\rangle, k)$
    stop $\langle b, a, m'\rangle, s'$
else if $path \equiv /startNegotiation$ then
    let $loginSessionToken := \nu_1$
    let $t := body[t]$
    let $ID_{rp} := [s'.\mathtt{rp}.id]G$
    let $PID_{rp} := [t]ID_{rp}$
    let $state := \mathtt{expectToken}$
    let $s'.\mathtt{loginSessions}[loginSessionToken] := \langle t, PID_{rp}, state\rangle$
    let $m' := \mathsf{enc_s}(\langle \mathtt{HTTPResp}, n, 200, \langle\rangle, \langle \mathtt{Cert_{RP}}, s'.\mathtt{IdPConfig}.Cert_{RP}\rangle\rangle, k)$
    stop $\langle b, a, m'\rangle, s'$
else if $path \equiv /uploadToken$ then
    let $loginSessions := s'.\mathtt{loginSessions}[body[\mathtt{loginSessionToken}]]$
    if $loginSessions \equiv \langle\rangle$ then
        stop $\langle\rangle, s'$
    end if
    if $loginSessions.\mathtt{state} \not\equiv expectToken$ then
        let $m' := \mathsf{enc_s}(\langle \mathtt{HTTPResp}, n, 200, \langle\rangle, \mathtt{Fail}\rangle, k)$
        stop $\langle b, a, m'\rangle, s'$
    end if
    let $s'.\mathtt{loginSessions} := s'.\mathtt{loginSessions} - body[loginSessionToken]$
    let $IDToken := body[\mathtt{IDToken}]$
    if $IDToken.\mathtt{PID_{rp}} \not\equiv loginSessions.\mathtt{PID_{rp}}$ then
        let $m' := \mathsf{enc_s}(\langle \mathtt{HTTPResp}, n, 200, \langle\rangle, \mathtt{Fail}\rangle, k)$
        stop $\langle b, a, m'\rangle, s'$
    end if
    if $\mathsf{checksig}(IDToken.\mathtt{ver}, \langle IDToken.\mathtt{PID_{rp}}, IDToken.\mathtt{PID_u}\rangle, s'.\mathtt{IdPConfig}.pubkey) \equiv \bot$ then
        let $m' := \mathsf{enc_s}(\langle \mathtt{HTTPResp}, n, 200, \langle\rangle, \mathtt{Fail}\rangle, k)$
        stop $\langle b, a, m'\rangle, s'$
    end if
    let $PID_u := IDToken.\mathtt{PID_u}$
    let $Acct := [loginSessions.\mathtt{t}]PID_u$
    let $s'.\mathtt{serviceTokens} := s'.\mathtt{serviceTokens} +^{\langle\rangle} Acct$
    let $m' := \mathsf{enc_s}(\langle \mathtt{HTTPResp}, n, 200, \langle\rangle, \mathtt{LoginSuccess}\rangle, k)$
    stop $\langle b, a, m'\rangle, s'$
end if
stop $\langle\rangle, s'$
```

B.13 Identity Providers

The identity provider IdP is a web server modeled as an atomic process (I, Z, R, s_0) with the addresses $I := \mathsf{addr}(\mathsf{IdP})$. Its initial state s_0 contains a list of its domains and (private) TLS keys, a list of users and identites, and a private key for signing IDTokens. Besides this, the full state of IdP further contains a list of used nonces, and information about active sessions.

IdP react to four types of requests:

First, they provide the `script_idp`, where a t will be chosen and following requests to IdP will be sent. IdP will transfer the data to RP by the communicating between two scripts `script_idp` and `script_rp` using `POSTMESSAGE`.

Second, they provide *IDToken* when receiving PID_{rp} and this PID_{rp} has already first. If not, IdPs will redirect to the login dialog.

After the user enter his username and password(secret) in the login dialog, a login request will send to /`authentication`. IdPs will check the parameters and set the login session.

The last type of requests IdPs react to is authorize requests with PID_{rp} and attribute scopes as parameters. After receving consent from browsers, IdPs will calculate PID_u and construct *IDToken*.

Formal description. In the following, we will first define the (initial) state of IdP formally and afterwards present the definition of the relation R.

To define the initial state, we will need a term that represents the "user database" of the IdP. We will call this term *userset*. This database defines, which secret is valid for which identity. It is encoded as a mapping of identities to secrets. For example, if the secret secret_1 is valid for the identites $\mathit{id}_1$and the secret secret_2 is valid for the identity id_2, the $\mathit{userset}^i$ looks as follows:

$$\mathit{userset} = [\mathit{id}_1.\mathtt{username}{:}\langle \mathit{id}_1, \mathit{secret}_1\rangle, \mathit{id}_2.\mathtt{username}{:}\langle \mathit{id}_2, \mathit{secret}_2\rangle]$$

We define *userset* as $\mathit{userset} = \langle\{\langle u.\mathtt{username}, \langle u, \mathit{secret} = \mathsf{secretOfID}(u)\rangle\rangle \mid u \in \mathsf{ID}^u\}\rangle$.

Definition 9. *A* state $s \in Z$ of the IdP *is a term of the form* $\langle \mathit{tlskeys}, \mathit{users}, \mathit{signkey}, \mathit{sessions}, \mathit{corrupt}\rangle$ *where* $\mathit{tlskeys} = \mathit{tlskeys}$, $\mathit{users} = \mathit{userset}$, $\mathit{signkey} \in \mathcal{N}$ *(the key used by the IdP to sign IDTokens),* $\mathit{sessions} \in \left[\mathcal{N} \times \mathcal{T}_{\mathcal{N}}\right]$, $\mathit{corrupt} \in \mathcal{T}_{\mathcal{N}}$.

An initial state s_0 of IdP *is a state of the form* $\langle \mathit{tlskeys}, \mathit{userset}, \mathsf{signkey}(\mathsf{IdP}), \langle\rangle, \bot\rangle$.

The relation R that defines the behavior of the IdP is defined as follows:

Algorithm 2 Relation of IdP R

```
Input: $\langle a, b, m\rangle, s$
let $s' := s$
if $s'.\mathtt{corrupt} \not\equiv \bot \vee m \equiv \mathtt{CORRUPT}$ then
    let $s'.\mathtt{corrupt} := \langle\langle a, f, m\rangle, s'.\mathtt{corrupt}\rangle$
    let $m' := d_V(s')$
    let $a' := \mathsf{IPs}$
    stop $\langle a', a, m'\rangle, s'$
end if
let $m_{dec}, k, k', \mathit{inDomain}$ such that
    ↪ $\langle m_{\text{dec}}, k\rangle \equiv \mathsf{dec_a}(m, k') \wedge \langle \mathit{inDomain}, k'\rangle \in s'.\mathtt{sslkeys}$
    ↪ if possible; otherwise stop $\langle\rangle, s'$
let $n, \mathit{method}, \mathit{path}, \mathit{parameters}, \mathit{headers}, \mathit{body}$ such that
    ↪ $\langle \mathtt{HTTPReq}, n, \mathit{method}, \mathit{path}, \mathit{parameters}, \mathit{headers}, \mathit{body}\rangle \equiv m_{dec}$
    ↪ if possible; otherwise stop $\langle\rangle, s'$
```

```
if $path \equiv /script$ then
    let $m' := \mathsf{enc_s}(\langle \texttt{HTTPResp}, n, 200, \langle\rangle, \texttt{script\_idp}\rangle, k)$
    stop $\langle b, a, m'\rangle, s'$
else if $path \equiv /authentication$ then
    let $username := body[\texttt{username}]$
    let $password := body[\texttt{password}]$
    if $password \not\equiv s'.\texttt{userset}[username].secret$ then
        let $m' := \mathsf{enc_s}(\langle \texttt{HTTPResp}, n, 200, \langle\rangle, \texttt{LoginFailure}\rangle, k)$
        stop $\langle b, a, m'\rangle, s'$
    end if
    let $sessionid := \nu_2$
    let $s'.\texttt{sessions}[sessionid] := username$
    let $setCookie := \langle \texttt{Set-Cookie}, \langle\langle \texttt{sessionid}, sessionid, \top, \top, \top\rangle\rangle\rangle$
    let $m' := \langle \texttt{HTTPResp}, n, 200, \langle setCookie\rangle, \texttt{LoginSucess}\rangle$
    stop $\langle b, a, m'\rangle, s'$
else if $path \equiv /reqToken$ then
    let $cookie := headers[\texttt{Cookie}]$
    if $cookie[\texttt{sessionid}] \equiv \langle\rangle$ then
        let $m' := \mathsf{enc_s}(\langle \texttt{HTTPResp}, n, 200, \langle\rangle, \texttt{Unauthenticated}\rangle, k)$
        stop $\langle b, a, m'\rangle, s'$
    end if
    let $sessionid := cookie[\texttt{sessionid}]$
    let $PID_{rp} := parameters[\texttt{PID}_{\texttt{rp}}]$
    if $s'.\texttt{sessions}[sessionid].IDToken[PID_{rp}] \equiv \langle\rangle$ then
        let $m' := \mathsf{enc_s}(\langle \texttt{HTTPResp}, n, 200, \langle\rangle, \texttt{Unauthorized}\rangle, k)$
        stop $\langle b, a, m'\rangle, s'$
    end if
    let $IDToken := s'.\texttt{sessions}[sessionid].IDToken[PID_{rp}]$
    let $m' := \mathsf{enc_s}(\langle \texttt{HTTPResp}, n, 200, \langle\rangle, IDToken\rangle, k)$
    stop $\langle b, a, m'\rangle, s'$
else if $path \equiv /authorize$ then
    let $cookie := headers[\texttt{Cookie}]$
    if $cookie[\texttt{sessionid}] \equiv \langle\rangle$ then
        let $m' := \mathsf{enc_s}(\langle \texttt{HTTPResp}, n, 200, \langle\rangle, \texttt{Unauthenticated}\rangle, k)$
        stop $\langle b, a, m'\rangle, s'$
    end if
    let $sessionid := cookie[\texttt{sessionid}]$
    let $PID_{RP} := parameters[\texttt{PID}_{\texttt{RP}}]$
    if $\texttt{IsValid}(PID_{RP}) \equiv \bot$ then
        let $m' := \mathsf{enc_s}(\langle \texttt{HTTPResp}, n, 200, \langle\rangle, \texttt{Fail}\rangle, k)$
        stop $\langle b, a, m'\rangle, s'$
    end if
    if $\texttt{IsInScope}(uid, body[\texttt{Attr}]) \equiv \bot$ then
        let $m' := \mathsf{enc_s}(\langle \texttt{HTTPResp}, n, 200, \langle\rangle, \texttt{Fail}\rangle, k)$
        stop $\langle b, a, m'\rangle, s'$
    end if
    let $u := s'.\texttt{sessions}[sessionid].u$
    let $ID_u := u.\texttt{id}$
    let $PID_u := [ID_u]PID_{rp}$
    let $content := \langle PID_{rp}, PID_u\rangle$
    let $ver := \mathsf{sig}(content, s'.\mathtt{signkey})$
    let $IDToken := \langle content, ver \rangle$
    let $s'.\mathtt{sessions}[IDTokens] := s'.\mathtt{sessions}[IDTokens] +^{\langle\rangle} \langle PID_{rp}, IDToken \rangle$
    let $m' := \mathsf{enc_s}(\langle \mathtt{HTTPResp}, n, 200, \langle\rangle, IDToken \rangle, k)$
    stop $\langle b, a, m' \rangle, s'$
end if
stop $\langle\rangle, s'$
```

B.14 UPPRESSO Scripts

As already mentioned in Appendix B.1, the set $\mathcal{S}$ of the web system $\mathcal{UWS} = (\mathcal{W}, \mathcal{S}, \mathsf{script}, E^0)$ consists of the scripts R^{att}, *script_rp*, *script_idp*, and with their string representations being `att_script`, `script_rp`, `script_idp`, and (defined by script).

In what follows, the scripts *script_rp* and *script_idp* are defined formally.

Relying Party Page (script_rp). As defined in SPRESSO, a script is a relation that takes a termas input and outputs a new term. The input term is provided by the browser. It contains the current internal state of the script (which we call *scriptstate* in what follows) and additional information containing all browser state information the script has access to, such as the input the script has obtained so far via XHRs and postMessages, information about windows, etc. The browser expects the output term to contain, among other information, the new internal *scriptstate*.

We first describe the structure of the internal scriptstate of the script *script_rp*.

Definition 10. *A* scriptstate s of *script_rp is a term of the form* $\langle$*phase*, *refXHR*$\rangle$, *where phase* $\in \mathbb{S}$, *refXHR* $\in \mathcal{N} \cup \{\perp\}$.

The initial scriptstate $initState_{rp}$ *of script_rp is* $\langle \mathtt{start}, \perp \rangle$.

We now specify the relation *script_rp* formally. We describe this relation by a non-deterministic algorithm.

Algorithm 3 Relation of *script_rp*

```
Input: $\langle tree, docnonce, scriptstate, scriptinputs, cookies, localStorage, sessionStorage,$
    $\hookrightarrow$ $ids, secret \rangle$
let $s' := scriptstate$
let $command := \langle\rangle$
let $origin := \mathsf{GETORIGIN}(tree, docnonce)$
let $RPDomain := origin.\mathtt{host}$
switch $s'.\mathtt{phase}$ do
    case start:
        let $url := \langle \mathtt{URL}, \mathtt{S}, RPDomain, \mathtt{/loginSSO}, \langle\rangle \rangle$
        let $command := \langle \mathtt{HREF}, url, \mathtt{\_BLANK}, \langle\rangle \rangle$
        let $s'.\mathtt{phase} := \mathtt{expectt}$
    case expectt:
        let $pattern := \langle \mathtt{POSTMESSAGE}, target, *, \langle \mathtt{t}, * \rangle \rangle$
        let $input := \mathsf{CHOOSEINPUT}(scriptinputs, pattern)$
    if $input \not\equiv \bot$ then
      let $t := \pi_2(\pi_4(input))$
      let $body := \langle\langle \mathtt{t}, t\rangle\rangle$
      let $command := \langle \mathtt{XMLHTTPREQUEST}, \mathsf{URL}^{RPDomain}_{\mathtt{/startNegotiation}}, \mathtt{POST}, body,$
       $\hookrightarrow$ $s'.\mathtt{refXHR}\rangle$
      let $s'.\mathsf{phase} := \mathtt{expectCert}$
    end if
  case $\mathtt{expectCert}$:
    let $pattern := \langle \mathtt{XMLHTTPREQUEST}, *, s'.\mathtt{refXHR}\rangle$
    let $input := \mathsf{CHOOSEINPUT}(scriptinputs, pattern)$
    if $input \not\equiv \bot$ then
      let $Cert_{rp} := \pi_2(input).\mathtt{Cert_{rp}}$
      let $IdPWindowNonce := \pi_1(\mathsf{SUBWINDOWS}(tree, docnonce)).\mathtt{nonce}$
      let $IdPOrigin := \mathsf{GETORIGIN}(tree, IdPWindowNonce)$
      let $command := \langle \mathtt{POSTMESSAGE}, IdPWindowNonce, \langle \mathtt{Cert}, Cert_{rp}\rangle,$
       $\hookrightarrow$ $IdPOrigin\rangle$
      let $s'.\mathsf{phase} := \mathtt{expectToken}$
    end if
  case $\mathtt{expectToken}$:
    let $pattern := \langle \mathtt{POSTMESSAGE}, target, *, \langle \mathtt{IDToken}, *\rangle\rangle$
    let $input := \mathsf{CHOOSEINPUT}(scriptinputs, pattern)$
    if $input \not\equiv \bot$ then
      let $IDToken := \pi_2(\pi_4(input))$
      let $body := \langle\langle \mathtt{IDToken}, IDToken\rangle\rangle$
      let $command := \langle \mathtt{XMLHTTPREQUEST}, \mathsf{URL}^{RPDomain}_{\mathtt{/uploadToken}}, \mathtt{POST}, body,$
       $\hookrightarrow$ $s'.\mathtt{refXHR}\rangle$
      let $s'.\mathsf{phase} := \mathtt{expectLoginResult}$
    end if
  case $\mathtt{expectLoginResult}$:
    let $pattern := \langle \mathtt{XMLHTTPREQUEST}, *, s'.\mathtt{refXHR}\rangle$
    let $input := \mathsf{CHOOSEINPUT}(scriptinputs, pattern)$
    if $input \not\equiv \bot$ then
      if $\pi_2(input) \equiv \mathtt{LoginSuccess}$ then
        let Load Homepage
      end if
    end if
end switch
stop $\langle s', cookies, localStorage, sessionStorage, command\rangle$
```

Identity Provider Page (script_idp).

Definition 11. *A* scriptstate s of *script_idp is a term of the form* $\langle$*phase, user, parameters*$\rangle$ *with phase* $\in \mathbb{S}$*, user* $\in \mathsf{ID} \cup \{\langle\rangle\} \in \mathcal{T}$ *and parameters* $\in \left[\mathbb{S} \times \mathcal{T}_{\mathcal{N}}\right]$*,. The* initial scriptstate *of script_idp is* $\langle \mathtt{start}, *, \langle\rangle\rangle$.

We now formally specify the relation of *script_idp*

Algorithm 4 Relation of *script_idp*

```
Input: $\langle tree, docnonce, scriptstate, scriptinputs, cookies, localStorage, sessionStorage,$
  $\hookrightarrow$ $ids, secret\rangle$
```

```
let $s' := \mathit{scriptstate}$
let $\mathit{command} := \langle\rangle$
let $\mathit{target} := \mathsf{OPENERWINDOW}(\mathit{tree}, \mathit{docnonce})$
let $\mathit{origin} := \mathsf{GETORIGIN}(\mathit{tree}, \mathit{docnonce})$
let $\mathit{IdPDomain} := \mathit{origin}.\mathtt{host}$
switch $s'.\mathsf{phase}$ do
    case $\mathit{start}$:
        let $t := \mathtt{random}()$
        let $\mathit{command} := \langle \mathtt{POSTMESSAGE}, \mathit{target}, \langle \mathtt{t}, t\rangle, \langle\rangle\rangle$
        let $s'.\mathtt{parameters}[t] := t$
        let $s'.\mathsf{phase} := \mathtt{expectCert}$
    case $\mathtt{expectCert}$:
        let $\mathit{pattern} := \langle \mathtt{POSTMESSAGE}, \mathit{target}, *, \langle \mathtt{Cert}, *\rangle\rangle$
        let $\mathit{input} := \mathsf{CHOOSEINPUT}(\mathit{scriptinputs}, \mathit{pattern})$
        if $\mathit{input} \not\equiv \bot$ then
            let $\mathit{Cert}_{rp} := \pi_2(\pi_4(\mathit{input}))$
            if $\mathsf{checksig}(\mathit{Cert}_{rp}.\mathtt{ver}, \mathit{Cert}_{rp}.\mathtt{content}, s'.\mathtt{IdPConfig}.\mathit{pubkey}) \equiv \top$ then
                let $s'.\mathtt{parameters}[\mathit{cert}] := \mathit{Cert}_{rp}$
                let $t := s'.\mathtt{parameters}[t]$
                let $\mathit{PID}_{rp} := [t]\mathit{Cert}_{rp}.\mathtt{content}[\mathit{ID}_{rp}]$
                let $s'.\mathtt{parameters}[\mathit{PID}_{rp}] := \mathit{PID}_{rp}$
                let $\mathit{body} := \langle\langle \mathtt{PID_{rp}}, \mathit{PID}_{rp}\rangle\rangle$
                let $\mathit{command} := \langle \mathtt{XMLHTTPREQUEST}, \mathsf{URL}^{\mathit{IdPDomain}}_{\mathtt{/reqToken}}, \mathtt{POST}, \mathit{body},$
                  $\hookrightarrow$ $s'.\mathtt{refXHR}\rangle$
                let $s'.\mathsf{phase} := \mathtt{expectReqToken}$
            end if
        end if
    case $\mathtt{expectReqToken}$:
        let $\mathit{pattern} := \langle \mathtt{XMLHTTPREQUEST}, *, s'.\mathtt{refXHR}\rangle$
        let $\mathit{input} := \mathsf{CHOOSEINPUT}(\mathit{scriptinputs}, \mathit{pattern})$
        if $\mathit{input} \not\equiv \bot$ then
            if $\pi_2(\mathit{input}) \equiv \mathtt{Unanthenticated}$ then
                let $s'.\mathsf{user} \leftarrow \mathit{ids}$
                let $\mathit{username} := s'.\mathsf{user}.\mathit{name}$
                let $\mathit{password} := \mathsf{secretOfID}(s'.\mathsf{user})$
                let $\mathit{body} := \langle\langle \mathtt{username}, \mathit{username}\rangle, \langle \mathtt{password}, \mathit{password}\rangle\rangle$
                let $\mathit{command} := \langle \mathtt{XMLHTTPREQUEST}, \mathsf{URL}^{\mathit{IdPDomain}}_{\mathtt{/authentication}}, \mathtt{POST}, \mathit{body},$
                  $\hookrightarrow$ $s'.\mathtt{refXHR}\rangle$
                let $s'.\mathsf{phase} := \mathtt{expectLoginResult}$
            else if $\pi_2(\mathit{input}) \equiv \mathtt{Unauthorized}$ then
                let $\mathit{PID}_{rp} := s'.\mathtt{parameters}[\mathit{PID}_{rp}]$
                let $\mathit{Attr} := \mathsf{GETPARAMETERS}(\mathit{tree}, \mathit{docnonce})[\mathtt{iaKey}]$
                let $\mathit{body} := \langle\langle \mathtt{PID_{rp}}, \mathit{PID}_{rp}\rangle, \langle \mathtt{Attr}, \mathit{Attr}\rangle\rangle$
                let $\mathit{command} := \langle \mathtt{XMLHTTPREQUEST}, \mathsf{URL}^{\mathit{IdPDomain}}_{\mathtt{/authorize}}, \mathtt{POST}, \mathit{body},$
                  $\hookrightarrow$ $s'.\mathtt{refXHR}\rangle$
                let $s'.\mathsf{phase} := \mathtt{expectToken}$
            else if  then
                let $\mathit{IDToken} := \pi_2(\mathit{input})[\mathtt{IDToken}]$
                let $\mathit{RPOringin} := \langle s'.\mathtt{parameters}[\mathit{cert}].\mathit{Content}[\mathtt{Enpt}], \mathtt{S}\rangle$
                let $\mathit{command} := \langle \mathtt{POSTMESSAGE}, \mathit{target}, \langle \mathtt{IDToken}, \mathit{IDToken}\rangle, \mathit{RPOrigin}\rangle$
                let $s'$.phase := stop
            end if
        end if
    case expectLoginResult:
        let $pattern$ := $\langle$XMLHTTPREQUEST, $*$, $s'$.refXHR$\rangle$
        let $input$ := CHOOSEINPUT($scriptinputs, pattern$)
        if $input \not\equiv \bot$ then
            if $\pi_2(input) \equiv$ LoginSuccess then
                let $PID_{rp}$ := $s'$.parameters[$PID_{rp}$]
                let $Attr$ := GETPARAMETERS($tree, docnonce$)[iaKey]
                let $body$ := $\langle\langle$PID$_{\mathtt{rp}}$, $PID_{rp}\rangle$, $\langle$Attr, $Attr\rangle\rangle$
                let $command$ := $\langle$XMLHTTPREQUEST, $\mathsf{URL}^{IdPDomain}_{\mathtt{/authorize}}$, POST, $body$,
                  ↪ $s'$.refXHR$\rangle$
                let $s'$.phase := expectToken
            end if
        end if
    case expectToken:
        let $pattern$ := $\langle$XMLHTTPREQUEST, $*$, $s'$.refXHR$\rangle$
        let $input$ := CHOOSEINPUT($scriptinputs, pattern$)
        if $input \not\equiv \bot$ then
            let $IDToken$ := $\pi_2(input)$[IDToken]
            let $RPOringin$ := $\langle s'$.parameters[$cert$].$Content$[Enpt], S$\rangle$
            let $command$ := $\langle$POSTMESSAGE, $target$, $\langle$IDToken, $IDToken\rangle$, $RPOrigin\rangle$
            let $s'$.phase := stop
        end if
end switch
stop $\langle s', cookies, localStorage, sessionStorage, command\rangle$
```

C Proof of Security

To state the security properties for UPPRESSO, we first define an *UPPRESSO web system for authentication analysis*. This web system is based on the UPPRESSO web system and only considers one network attacker (which subsumes all web attackers and further network attackers).

Definition 12. *Let* $\mathcal{UWS}^{auth} = (\mathcal{W}, \mathcal{S}, \mathsf{script}, E^0)$ *an UPPRESSO web system. We call* $\mathcal{UWS}^{auth}$ *an* UPPRESSO web system for authentication analysis *iff* $\mathcal{W}$ *contains only one network attacker process* attacker *and no other attacker processes (i.e.,* $\mathsf{Net} = \{\mathsf{attacker}\}$*,* $\mathsf{Web} = \emptyset$*).*

The security properties for UPPRESSO are formally defined as follows. First note that every *Acct* recorded in RP was calculated by RP as the result of an HTTPS `POST` request m. We refer to m as the *request corresponding to Acct*.

In the following definition, when we say a browser $b \in \mathsf{B}$ owns *Acct*, we holds that for some RP $r \in \mathsf{RP}$ that calculate it and an identity $u \in \mathsf{ID}$ with $\mathsf{ownerOfID}(u) = b$.

$$Acct = acct^u[\mathsf{dom}(r)]$$

We now define the similar security properties as the definition 52 in SPRESSO.

Definition 13. *Let $\mathcal{UWS}^{auth}$ be an UPPRESSO web system for authentication analysis. We say that $\mathcal{UWS}^{auth}$* is secure *if for every run ρ of $\mathcal{UWS}^{auth}$, every state (S^j, E^j, N^j) in ρ, every $r \in \mathsf{RP}$ that is honest in S^j, every RP service token of the form Acct recorded in $S^j(r)$.*`serviceTokens`*, the following two conditions are satisfied:*

(A) *If Acct is derivable from the attackers knowledge in S^j (i.e., $Acct \in d_\emptyset(S^j(\mathsf{attacker}))$), then it follows that the browser b owning Acct is fully corrupted in S^j (i.e., the value of isCorrupted is* `FULLCORRUPT`*) or the only IdP is dishonest (in S^j).*

(B) *If the request corresponding to Acct was sent by some $b \in \mathsf{B}$ which is honest in S^j, then b owns Acct.*

To prove Theorem 1 in section 5.1, we are going to prove the following Lemmas.

Lemma 1. *If in the processing step $s_i \to s_{i+1}$ of a run ρ of $\mathcal{UWS}^{auth}$ an honest relying party r (I) emits an HTTPS request of the form*

$$m = \mathsf{enc_a}(\langle req, k\rangle, \mathsf{pub}(k'))$$

(where req is an HTTP request, k is a nonce (symmetric key), and k' is the private key of some other DY process u), and (II) in the initial state s_0 the private key k' is only known to u, and (III) u never leaks k', then all of the following statements are true:

1. *There is no state of $\mathcal{UWS}^{auth}$ where any party except for u knows k', thus no one except for u can decrypt req.*
2. *If there is a processing step $s_j \to s_{j+1}$ where the RP r leaks k to $\mathcal{W} \setminus \{u, r\}$ there is a processing step $s_h \to s_{h+1}$ with $h < j$ where u leaks the symmetric key k to $\mathcal{W} \setminus \{u, r\}$ or r is corrupted in s_j.*
3. *The value of the host header in req is the domain that is assigned the public key $\mathsf{pub}(k')$ in RP's keymapping s_0.*`keyMapping` *(in its initial state).*
4. *If r accepts a response (say, m') to m in a processing step $s_j \to s_{j+1}$ and r is honest in s_j and u did not leak the symmetric key k to $\mathcal{W} \setminus \{u, r\}$ prior to s_j, then u created the HTTPS response m' to the HTTPS request m, i.e., the nonce of the HTTP request req is not known to any atomic process p, except for the atomic DY processes r and u.*

Lemma 2. *In a run ρ of $\mathcal{UWS}^{auth}$, for every state $s_j \in \rho$, every RP $r \in \mathsf{RP}$ that is honest in s_j, every $\langle nonce, Acct\rangle \in^{\langle\rangle} S^j(r)$.*`serviceTokens`*, the following properties hold:*

1. *There exists exactly one $l' < j$ such that there exists a processing step in ρ of the form*

$$s_{l'} \xrightarrow[r \to \langle\langle a', f', m'\rangle\rangle]{e' \to r} s_{l'+1}$$

with e' being some events, a' and f' being addresses and m' being a service token response for Acct.

2. *There exists exactly one $l < j$ such that there exists a processing step in ρ of the form*

$$s_l \xrightarrow[r \to e]{\langle a, f, m\rangle \to r} s_{l+1}$$

with e being some events, a and f being addresses and m being a service token request for Acct.

3. *The processing steps from (1) and (2) are the same, i.e., $l = l'$.*

4. *The service token request for Acct, m in (2), is an HTTPS message of the following form:*

$$\mathsf{enc_a}(\langle\langle \mathtt{HTTPReq}, n_{req}, \mathtt{POST}, d_r, /\mathtt{authorize}, x, h, b\rangle, k\rangle, \mathsf{pub}(\mathsf{tlskey}(d_r)))$$

for $d_r \in \mathsf{dom}(r)$, some terms x, h, n_{req}, and a dictionary b such that

$$b[\mathtt{IDToken}] \equiv \langle PID_{rp}, PID_u, ver\rangle$$

with

$$PID_{rp} \equiv [S^l(r).\mathtt{loginSessions}[t]][S^l(r).\mathtt{rp}.id]G,$$
$$PID_u \equiv [u]PID_{rp},$$
$$ver \equiv \mathsf{sig}(\langle PID_{rp}, PID_u\rangle, k_{sign})$$

for some nonces u, and k_{sign}.

5. *If the IdP i is honest, we have that $k_{sign} = S^l(i).\mathtt{signkey}$.*

We define the Lemma 1 and 2, which prove that the data transmitted through HTTPS is secure and the IdP's public key used for generating IDToken is secure. In UPPRESSO, only the single IdP is trusted, so that the public key is guaranteed to be always trusted. Therefore, we can also follow the proofs in SPRESSO.

C.1 Proof of Property A

Then we prove the Property A is satisfied in UPPRESSO. As stated above, the Property A is defined as follows:

Definition 14. *Let $\mathcal{UWS}^{auth}$ be an UPPRESSO web system for authentication analysis. We say that $\mathcal{UWS}^{auth}$* is secure (with respect to Property A) *if for every run ρ of $\mathcal{UWS}^{auth}$, every state (S^j, E^j, N^j) in ρ, every $r \in \mathsf{RP}$ that is honest in S^j, every RP service token of the form $\langle nonce, Acct\rangle$ recorded in $S^j(r)$.*`serviceTokens` *and derivable from the attackers knowledge in S^j (i.e., $\langle nonce, Acct\rangle \in d_\emptyset(S^j(\mathsf{attacker}))$), it follows that the browser b owning Acct is fully corrupted in S^j (i.e., the value of isCorrupted is* `FULLCORRUPT`*) or the IdP is dishonest.*

Same as the proof in SPRESSO, we want to show that every UPPRESSO web system is secure with regard to Property A and therefore assume that there exists an UPPRESSO web system that is not secure. We will lead this to a contradication and thereby show that all UPPRESSO web systems are secure (with regard to Property A).

In detail, we assume: *There exists an UPPRESSO web system $\mathcal{UWS}^{auth}$, a run ρ of $\mathcal{UWS}^{auth}$, a state $s_j = (S^j, E^j, N^j)$ in ρ, a RP $r \in \mathsf{RP}$ that is honest in S^j, an RP service token of the form $\langle nonce, Acct\rangle$ recorded in $S^j(r)$.*`serviceTokens` *and derivable from the attackers knowledge in S^j (i.e., $Acct \in d_\emptyset(S^j(\mathsf{attacker}))$), and the browser b owning i is not fully corrupted and IdP is honest (in S^j).*

We now proceed to proof that this is a contradiction. First, we can see that for $\langle n, Acct\rangle$ and s_j, the conditions in Lemma 2 are fulfilled, i.e., a service token request m and a service token response m' to/from r exist, and m' is of form shown in Lemma 2 (4). Let $I := \mathsf{governor}(Acct)$. We know that I is an honest IdP. As such, it never leaks its signing key (see Algorithm 2). Therefore, the signed subterm $Content := \langle PID_{rp}, PID_u\rangle$, $ver := \mathsf{sig}(\langle PID_{rp}, PID_u\rangle, k_{sign})$ and $IDToken := \langle Content, ver\rangle$ had to be created by the IdP I. An (honest) IdP creates signatures only in Line 60 of Algorithm 2.

Lemma 3. *Under the assumption above, only the browser b can issue a request req (say, m_{attr})that triggers the IdP I to create the signed term IDToken. The request was sent by b over HTTPS using I's public HTTPS key.*

Proof. We have to consider two cases for the request m_{attr}:

(A). First, if the user is not logged in with the identity u at I (i.e., the browser b has no session cookie that carries a nonce which is a session id at I for which the identitiy u is marked as being logged in, compare Line 42 of Algorithm 2), then the request has to carry (in the request body) the password matching the identity u ($\mathsf{secretOfID}(u)$) to the path `/authentication` to retrieve the session cookie. This secret is only known to b initially. Depending on the corruption status of b, we can now have two cases:

a) If b is honest in s_j, it has not sent the secret to any party except over HTTPS to I (as defined in the definition of browsers).

b) If b is close-corrupted, it has not sent it to any other party while it was honest (case a). When becoming close-corrupted, it discarded the secret.

I.e., the secret has been sent only to I over HTTPS or to nobody at all. The IdP I cannot send it to any other party. Therefore we know that only the browser b can send the request m_{attr} in this case.

(B). Second, if the user is logged in for the identity i at I, the browser provides a session id to I that refers to a logged in session at I. This session id can only be retrieved from I by logging in, i.e., case (A) applies, in particular, b has to provide the proper secret, which only itself and I know (see above). The session id is sent to b in the form of a cookie, which is set to secure (i.e., it is only sent back to I over HTTPS, and therefore not derivable by the attacker) and httpOnly (i.e., it is not accessible by any scripts). The browser b sends the cookie only to I. The IdP I never sends the session id to any other party than b. The session id therefore only leaks to b and I, and never to the attacker. Hence, the browser b is the only atomic DY process which can send the request m_{attr} in this case.

We can see that in both cases, the request was sent by b using HTTPS and I's public key: If the browser would intend to sent the request without encryption, the request would not contain the password in case (A) or the cookie in case (B). The browser always uses the "correct" encryption key for any domain (as defined in $\mathcal{UWS}^{auth}$). □

Lemma 4. *In the browser b, the request m_{attr} was triggered by script_idp loaded from the origin $\langle d, S\rangle$ for some $d \in \mathtt{dom}(I)$.*

Proof. First, $\langle d, \mathsf{S}\rangle$ for some $d \in \mathtt{dom}(I)$ is the only origin that has access to the secret $\mathsf{secretOfID}(u)$ for the identity u (as defined in Appendix B.11).

With the general properties defined in [1] and the definition of Identity Providers in Appendix B.13, in particular their property that they only send out one script, *script_idp*, we can see that this is the only script that can trigger a request containing the secret. □

Lemma 5. *In the browser b, the script script_idp receives the response to the request m_{attr} (and no other script), and at this point, the browser is still honest.*

Proof. From the definition of browser corruption, we can see that the browser b discards any information about pending requests in its state when it becomes close-corrupted, in particular any SSL keys. It can therefore not decrypt the response if it becomes close-corrupted before receiving the response.

The rest follows from the general properties defined in [1]. □

We now know that only the script *script_idp* received the response containing the IDToken. For the following lemmas, we will assume that the browser b is honest. In the other case (the browser is close-corrupted), the IA ia and any information about pending HTTPS requests (in particular, any decryption keys) would be discarded from the browser's state (as seen in the proof for Lemma 5). This would be a contradiction to the assumption (which requires that the IDToken arrived at the RP).

Lemma 6. *The script script_idp forwards the IDToken only to the script script_rp loaded from the origin $\langle d_r, \mathsf{S}\rangle$.*

Proof. It is clear that, the IDToken held by the honest *script_idp* is only sent to the origin $\langle Cert_{rp}.Enpt_{rp}, \mathsf{S}\rangle$, while the $IDToken.PID_{rp} \equiv [t]Cert_{rp}.ID_{rp}$, and t is the one-time random number. The relation of $Cert_{rp}.ID_{rp}$ and $Cert_{rp}.Enpt_{rp}$ is guaranteed by the signature $Cert_{rp}.ver$ generated by IdP I. The process is shown at Line 69 Algorithm 4. □

Lemma 7. *From the RP document, the IDToken is only sent to the RP r and over HTTPS*

Proof. It is proved that *script_rp* of the origin $\langle Cert_{rp}.Enpt_{rp}, \mathsf{S}\rangle$ would only sent to the corresponding RP r, which is shown in Algorithm 3. □

The proofs show that the IDToken is only sent to the honest browser and target RP. It cannot be known to the attacker or any corrupted party, as none of the listed parties leak it to any corrupted party or the attacker. Above proofs can be reduced to the Confidentiality and Integrity Properties, simply described as the Theorem 3 and 4 in section 5.2.

These proofs are enough for SPRESSO system to show its security, however, they are not enough for UPPRESSO. So far, the proofs only guarantee that the $IDToken$ must be sent to the target RP. In SPRESSO, as the *tag* can be only decrypted to unique *Domain*, the target RP must be the honest RP (the target of an adversary). However, in UPPRESSO, while an RP receives an $IDToken$, he may try to use this token to login another honest RP, as long as he can find the $t^{adversary}$ satisfied $IDToken.PID_{RP} \equiv [t^{adversary}]ID_{RP}^{honest}$. Therefore, the following Lemma should be proved.

Lemma 8. *The $t^{adversary}$ is not derivable from the attackers knowledge in S^j (i.e., $\langle IDToken,\ Acct\rangle \in d_{\emptyset}(S^j(\mathsf{attacker}))$), which satisfies that $IDToken.PID_{RP} \equiv [t^{adversary}]ID_{RP}^{honest}$.*

Proof. This Lemma can be proved by the Theorem 1 in section 5.2, as the RP Designation Property. □

Therefore, there is a contradication to the assumption, where we assumed that $Acct \in d_{\emptyset}(S^j(\mathsf{attacker}))$. This shows every $\mathcal{UWS}^{auth}$ is secure in the sense of Property A.

C.2 Proof of Property B

As stated above, Property B is defined as follows:

Definition 15. *Let $\mathcal{UWS}^{auth}$ be an UPPRESSO web system. We say that $\mathcal{UWS}^{auth}$* is secure (with respect to Property B) *if for every run ρ of $\mathcal{UWS}^{auth}$, every state (S^j, E^j, N^j) in ρ, every $r \in \mathsf{RP}$ that is honest in S^j, every RP service token of the form Acct recorded in $S^j(r)$.*`serviceTokens`*, with the request corresponding to Acct sent by some $b \in \mathsf{B}$ which is honest in S^j, b owns Acct.*

First we call the request corresponding to *Acct* (or service token request) m and its response m', and we refer to the state of $\mathcal{UWS}^{auth}$ in the run ρ where r processes m by s_l. We are going to prove the $IDToken$ uploaded by honest b can only be related with the *Acct* owned by b.

Lemma 9. *For every $IDToken$ uploaded by honest b during authentication, the honest $r \in RP$ can always derive the service token of the form $\langle IDToken, Acct\rangle$ recorded in $S^j(r)$.*`serviceTokens`*, where b owns Acct.*

Proof. Following the definiton of browser scripts, we know that m was sent by *script_rp*. The RP accepts the user's identity at line 46 in Algorithm 1. And the identity is generated at Line 45, based on the PID_u retrieved from the IDToken and the trapdoor t^{-1}. The t^{-1} is generated and set at Line 18 which is never changed. The IDToken is issued at Line 60 in Algorithm 2. The IdP generates the PID_u based on the PID_{rp} and ID_u related to $b \in \mathsf{B}$.

An attacker may allure the honest user to upload the IDToken $\in d_{\emptyset}(S^j(\texttt{attacker}))$ to honest $r \in \mathsf{RP}$, so that there may be $Acct \in d_{\emptyset}(S^j(\texttt{attacker}))$. However, while b has already negotiated the PID_{rp} with r, the opener of the *script_idp* must be the *script_rp*. As the t generated at Line 18, Algorithm 4, and PID_{RP} generated at Line 20 in Algorithm 4. The t is only sent to *script_rp* at Line 9 in Algorithm 4, and the *script_rp* receives it at Line 14 in Algorithm 3. The PID_{RP} is sent to the honest IdP at Lines 58 in Algorithm 4, which is used for generating the $IDToken$.

For every IDToken sent by honest b and honest r, there must be $IDToken.PID_{rp} \equiv [t]Cert_{rp}.ID_{rp}$, $IDToken.PID_u \equiv [ID_u]IDToken.PID_u$ and $Acct \equiv [t^{-1}]IDToken.PID_u$. According to the proof of Theorem 2 in section 5.2, the *Acct* must be owned by honest b ($Acct \equiv [ID_U]S^j(r).ID_{RP}$, where ID_U owned by b), which can be define as the User Identification Property. □

With the above proofs, we now can guarantee that every $\mathcal{UWS}^{auth}$ system satisfies the requirements in Definition 15, therefore $\mathcal{UWS}^{auth}$ must be secure of Property B.

D Proof of Privacy against IdP-based Login Tracing

In our privacy analysis, we show that an identity provider in UPPRESSO cannot learn where its users log in. We formalize this property as an indistinguishability property: an identity provider (modeled as a web attacker) cannot distinguish between a user logging in at one relying party and the same user logging in at a different relying party.

We will here first describe the precise model that we use for privacy. After that, we define an equivalence relation between configurations, which we will then use in the proof of privacy.

D.1 Formal Model of UPPRESSO for Privacy Analysis

Definition 16 (Challenge Browser)**.** *Let dr some domain and $b(dr)$ a DY process. We call $b(dr)$ a* challenge browser *iff b is defined exactly the same as a browser with two exceptions: (1) the state contains one more property, namely challenge, which initially contains the term $\top$. The broswer's algorithm is extended by the following at its very beginning: It is checked if a message m is addressed to the domain* `CHALLENGE` *(which we call the challenger domain). If m is addressed to this domain and no other message m' was addressed to this domain before (i.e., challenge $\not\equiv \bot$), then m is changed to be addressed to the domain dr and challenge is set to $\bot$ to recorded that a message was addressed to* `CHALLENGE`*.*

Definition 17 (Deterministic DY Process)**.** *We call a DY process $p = (I^p, Z^p, R^p, s_0^p)$* deterministic *iff the relation R^p is a (partial) function.*

We call a script R_{script} deterministic *iff the relation R_{script} is a (partial) function.*

Definition 18 (UPPRESSO Web System for Privacy Analysis)**.** *Let $\mathcal{UWS} = (\mathcal{W}, \mathcal{S}, \mathsf{script}, E^0)$ be an UPPRESSO web system with $\mathcal{W} = \mathsf{Hon} \cup \mathsf{Web} \cup \mathsf{Net}$, $\mathsf{Hon} = \mathsf{B} \cup \mathsf{RP} \cup \mathsf{IDP} \cup \mathsf{DNS}$. (as described in Appendix B.1). $\mathsf{RP} = \{r_1, r_2\}$, r_1 and r_2 two (honest) relying parties, dns an honest DNS server. Let $\mathsf{attacker} \in \mathsf{Web}$ be some web attacker. Let dr be a domain of r_1 or r_2 and $b(dr)$ a challenge browser. Let $\mathsf{Hon}' := \{b(dr)\} \cup \mathsf{RP} \cup \mathsf{DNS}$, $\mathsf{Web}' := \mathsf{Web}$, and $\mathsf{Net}' := \emptyset$ (i.e., there is no network attacker). Let $\mathcal{W}' := \mathsf{Hon}' \cup \mathsf{Web}' \cup \mathsf{Net}'$. Let $\mathcal{S}' := \mathcal{S} \setminus \{\mathtt{script\_idp}\}$ and script' be accordingly. We call $\mathcal{UWS}^{priv}(dr) = (\mathcal{W}', \mathcal{S}', \mathsf{script}', E^0, \mathsf{attacker})$ an* UPPRESSO web system for privacy analysis *iff the domain dr_1 the only domain assigned to r_1, and dr_2 the only domain assigned to r_2. The browser $b(dr)$ owns exactly one identity and this identity is governed by some attacker. All honest parties (in Hon) are not corruptible, i.e., they ignore any* `CORRUPT` *message. Identity providers are assumed to be dishonest, and hence, are subsumed by the web attackers (which govern all identities). the relying parties already know some public key to verify UPPRESSO identity assertions from all domains known in the system and they do not have to fetch them from IdP.*

As all parties in an UPPRESSO web system for privacy analysis are either web attackers, browsers, or deterministic processes and all scripting processes are either the attacker script or deterministic, it is easy to see that in UPPRESSO web systems for privacy analysis with configuration (S, E, N) a command ζ induces at most one processing step. We further note that, under a given infinite sequence of nonces N^0, all schedules σ induce at most one run $\rho = ((S^0, E^0, N^0), \ldots, (S^i, E^i, N^i), \ldots, (S^{|\sigma|}, E^{|\sigma|}, N^{|\sigma|}))$ as all of its commands induce at most one processing step for the i-th configuration.

We will now define our privacy property for UPPRESSO:

Definition 19 (IdP-Privacy)**.** *Let*

$$\mathcal{UWS}_1^{priv} := \mathcal{UWS}^{priv}(dr_1) = (\mathcal{W}_1, \mathcal{S}, \mathsf{script}, E^0, \mathsf{attacker}_1) \text{ and}$$
$$\mathcal{UWS}_2^{priv} := \mathcal{UWS}^{priv}(dr_2) = (\mathcal{W}_2, \mathcal{S}, \mathsf{script}, E^0, \mathsf{attacker}_2)$$

be UPPRESSO web systems for privacy analysis. Further, we require $\mathsf{attacker}_1 = \mathsf{attacker}_2 =: \mathsf{attacker}$ *and for* $b_1 := b(dr_1)$*,* $b_2 := b(dr_2)$ *we require* $S(b_1) = S(b_2)$ *and* $\mathcal{W}_1 \setminus \{b_1\} = \mathcal{W}_2 \setminus \{b_2\}$ *(i.e., the web systems are the same up to the parameter of the challenge browsers). We say that* $\mathcal{UWS}^{priv}$ *is* IdP-private *iff* $\mathcal{UWS}_1^{priv}$ *and* $\mathcal{UWS}_2^{priv}$ *are indistinguishable.*

D.2 Definition of Equivalent Configurations

Let $\mathcal{UWS}_1^{priv} = (\mathcal{W}_1, \mathcal{S}, \mathsf{script}, E^0, \mathsf{attacker})$ and $\mathcal{UWS}_2^{priv} = (\mathcal{W}_2, \mathcal{S}, \mathsf{script}, E^0, \mathsf{attacker})$ be UPPRESSO web systems for privacy analysis. Let (S_1, E_1, N_1) be a configuration of $\mathcal{UWS}_1^{priv}$ and (S_2, E_2, N_2) be a configuration of $\mathcal{UWS}_2^{priv}$.

Definition 20 (Proto-Tags)**.** *We call a term of the form* $[t]R$ *with the variable* R *as a placeholder for an* ID_{rp}*, and* t *some nonces a* proto-tag*.*

Definition 21 (Term Equivalence up to Proto-Tags)**.** *Let* $\theta = \{a_1, \ldots, a_l\}$ *be a finite set of proto-tags. Let* t *and* t' *be terms. We call* t_1 *and* t_2 term-equivalent under a set of proto-tags θ *iff there exists a term* $\tau \in \mathcal{T}_{\mathcal{N}}(\{x_1, \ldots, x_l\})$ *such that* $t_1 = (\tau[a_1/x_1, \ldots, a_l/x_l])[ID_{dr_1}/R]$ *and* $t_2 = (\tau[a_1/x_1, \ldots, a_l/x_l])[ID_{dr_2}/R]$*. We write* $t_1 \rightleftharpoons_\theta t_2$*.*

We say that two finite sets of terms D *and* D' *are* term-equivalent under a set of proto-tags θ *iff* $|D| = |D'|$ *and, given a lexicographic ordering of the elements in* D *of the form* $(d_1, \ldots, d_{|D|})$ *and the elements in* D' *of the form* $(d'_1, \ldots, d_{|D'|})$*, we have that for all* $i \in \{1, \ldots, |D|\}$*:* $d_i \rightleftharpoons_\theta d'_i$*. We then write* $D \rightleftharpoons_\theta D'$*.*

Definition 22 (Equivalence of HTTP Requests)**.** *Let* m_1 *and* m_2 *be (potentially encrypted) HTTP requests and* $\theta = \{a_1, \ldots, a_l\}$ *be a finite set of proto-tags. We call* m_1 *and* m_2 δ-equivalent under a set of proto-tags θ *iff* $m_1 \rightleftharpoons_\theta m_2$ *or all subterms are equal with the following exceptions:*

1. *the Host value and the Origin/Referer headers in both requests are the same except that the domain* dr_1 *in* m_1 *can be replaced by* dr_2 *in* m_2*,*

2. *the HTTP body* g_1 *of* m_1 *and the HTTP body* g_2 *of* m_2 *are (I) term-equivalent under* θ*, (II) for* $j \in \{1, 2\}$ *if* $g_j[\mathtt{IDToken}] \sim \langle PID_{dr_j}, [*]PID_{dr_j}, \mathsf{sig}(\langle PID_{dr_j}, [*]PID_{dr_j}\rangle, *)\rangle$ *and the origin (HTTP header) of HTTP message in* m_j *is* $\langle dr_j, \mathtt{S}\rangle$ *then the receiver of this message is* r_j*, and (III) if* g_1 *contains a dictionary key* `loginSessionToken` *then there exists an* $l' \in L$ *such that* $g_1[\mathtt{loginSessionToken}] \equiv l'$*, and*

3. *if m_1 is an encrypted HTTP request then and only then m_2 is an encrypted HTTP request and the keys used to encrypt the requests have to be the correct keys for dr_1 and dr_2 respectively.*

We write $m_1 \bumpeq_\theta m_2$.

Definition 23 (Extracting Entries from Login Sessions)**.** *Let t_1, t_2 be dictionaries over $\mathcal{N}$ and $\mathcal{T}_{\mathcal{N}}$, θ be a finite set of proto-tags, and d a domain. We call t_1 and t_2* η-equivalent *iff t_2 can be constructed from t_1 as follows: For every proto-tag $a \in \theta$, we remove the entry identified by the dictionary key i for which it holds that $\pi_4(t_1[i]) \equiv a[ID_r/R]$, if any. We denote the set of removed entries by D. We write $t_1 \trianglerighteq^\theta_r (t_2, D)$.*

Definition 24. *Let a be a proto-tag, S_1 and S_2 be states of UPPRESSO web systems for privacy analysis, and l a nonce. We call l a login session token for the proto-tag a, written $l \in \mathsf{loginSessionTokens}(a, S_1, S_2)$ iff for any $i \in \{1, 2\}$ and any $j \in \{1, 2\}$ we have that $\pi_4(S_i(r_j).\mathtt{loginSessions}[l]) = a[ID_{dr_j}/R]$.*

Definition 25 (Equivalence of States)**.** *Let θ be a set of proto-tags and H be a set of nonces. Let $T := \{t \mid [t]R \in \theta\}$. We call S_1 and S_2* γ-equivalent under (θ, H) *iff the following conditions are met:*

1. *$S_1(\mathsf{dns}) = S_2(\mathsf{dns})$, and*

2. *$S_1(\mathsf{r}_1)$ equals $S_2(\mathsf{r}_1)$ except for the subterms* `loginSessions` *and* `serviceTokens`*, and*

3. *$S_1(\mathsf{r}_2)$ equals $S_2(\mathsf{r}_2)$ except for the subterms* `loginSessions` *and* `serviceTokens`*, and*

4. *for two sets of terms D and D': $S_1(\mathsf{r}_1).\mathtt{loginSessions} \trianglerighteq^\theta_{dr_1} (S_2(\mathsf{r}_1).\mathtt{loginSessions}, D)$, $S_2(\mathsf{r}_2).\mathtt{loginSessions} \trianglerighteq^\theta_{dr_2} (S_1(\mathsf{r}_2).\mathtt{loginSessions}, D')$, and $D \rightleftharpoons_\theta D'$, and*

5. *$\forall t \in T$: $t \notin d_\emptyset(\bigcup_{i \in \{1,2\},\ A \in \mathsf{Web} \cup \mathsf{Net}} S_i(A))$*

6. *for each attacker A: $S_1(A) \rightleftharpoons_\theta S_2(A)$, and*

7. *for all $a \in \theta$ and all attackers A we have that $\nexists\, l \in \mathsf{loginSessionTokens}(a, S_1, S_2)$ such that l is a subterm of $S_1(A)$ or $S_2(A)$.*

8. *$S_1(b_1)$ equals $S_2(b_2)$ except for for the subterms* `challenge`*,* `windows` *and we have that*

   (a) *$S_1(b_1).\mathtt{challenge} = dr_1 \wedge S_2(b_2).\mathtt{challenge} = dr_2$ or $S_1(b_1).\mathtt{challenge} = S_2(b_2).\mathtt{challenge} = \bot$, and*

   (b) *$S_1(b_1).\mathtt{windows}$ equals $S_2(b_2).\mathtt{windows}$ with the exception of the subterms* `location`*,* `referrer`*,* `scriptstate`*, and* `scriptinputs` *of some document terms pointed to by $\mathsf{Docs}^+(S_1(b_1)) = \mathsf{Docs}^+(S_2(b_2)) =: J$. For all $j \in J$ we have that:*

i. *there is no $t \in T$ such that*

$$t \in d_{\mathcal{N} \setminus \{t\}}(\{S_1(b_1).j.\mathtt{location}, S_2(b_2).j.\mathtt{location}, \\ S_1(b_1).j.\mathtt{referrer}, S_2(b_2).j.\mathtt{referrer}\})$$

ii. *if $S_1(b_1).j.\mathtt{origin} \in \{\langle dr_1, \mathtt{S}\rangle, \langle dr_2, \mathtt{S}\rangle\}$ then $S_1(b_1).j.\mathtt{script} \equiv \mathtt{script\_rp}$ and*

A. *$S_1(b_1).j.\mathtt{location}$ and $S_2(b_2).j.\mathtt{location}$ are term-equivalent under θ except for the host part, which is either equal or dr_1 in b_1 and dr_2 in b_2, and*

B. *$S_1(b_1).j.\mathtt{referrer}$ and $S_2(b_2).j.\mathtt{referrer}$ are term-equivalent under θ except for the host part, which is either equal or dr_1 in b_1 and dr_2 in b_2, and*

C. *$S_1(b_1).j.\mathtt{scriptstate} \rightleftharpoons_\theta S_2(b_2).j.\mathtt{scriptstate}$ and if $\exists\, l \in L$ such that l is a subterm of $S_1(b_1).j.\mathtt{scriptstate}$, then $S_1(b_1).j.\mathtt{location.host} \equiv dr_1$ and $S_2(b_2).j.\mathtt{location.host} \equiv dr_2$, and*

D. *if $\exists\, l \in L$ such that l is a subterm of $S_1(b_1).j.\mathtt{scriptinputs}$, then $S_1(b_1).j.\mathtt{location.host} \equiv dr_1$ and $S_2(b_2).j.\mathtt{location.host} \equiv dr_2$, and*

iii. *if $S_1(b_1).j.\mathtt{origin} \notin \{\langle dr_1, \mathtt{S}\rangle, \langle dr_2, \mathtt{S}\rangle\}$ then $S_1(b_1).j.\mathtt{script} \equiv \mathtt{script\_idp}$ and*

A. *$S_1(b_1).j.\mathtt{location} \rightleftharpoons_\theta S_2(b_2).j.\mathtt{location}$, and*

B. *$S_1(b_1).j.\mathtt{referrer} \rightleftharpoons_\theta S_2(b_2).j.\mathtt{referrer}$, and*

C. *$S_1(b_1).j.\mathtt{scriptstate} \rightleftharpoons_\theta S_2(b_2).j.\mathtt{scriptstate}$, and*

D. *$S_1(b_1).j.\mathtt{scriptinputs} \rightleftharpoons_\theta S_2(b_2).j.\mathtt{scriptinputs}$, and*

E. *$\forall t \in T$: t is not contained in any subterm of $S_1(b_1).j.\mathtt{scriptstate}$ except for $S_1(b_1).j.\mathtt{scriptstate}.parameters[\mathtt{t}]$, and*

F. *$\nexists\, l \in L$ such that l is a subterm of $S_1(b_1).j.\mathtt{scriptstate}$ or of $S_1(b_1).j.\mathtt{scriptinputs}$, and*

(c) *for $x \in \{\mathtt{cookies}, \mathtt{localStorage}, \mathtt{sessionStorage}, \mathtt{sts}\}$ we have that $S_1(b_1).x \rightleftharpoons_\theta S_2(b_2).x$. For the domains dr_1 and dr_2 there are no entries in the subterms x.*

Definition 26 (Equivalence of Events)**.** *Same as Definition 80 in SPRESSO except that the forth condition in Definition 80 in SPRESSO is not applicable.*

Definition 27 (Equivalence of Configurations)**.** *We call (S_1, E_1, N_1) and (S_2, E_2, N_2) α-*equivalent *iff there exists a set of proto-tags θ and a set of nonces H such that S_1 and S_2 are γ-equivalent under (θ, H), E_1 and E_2 are β-equivalent under (θ, L, H) for $L := \bigcup_{a \in \theta} \mathsf{loginSessionTokens}(a, S_1, S_2)$, and $N_1 = N_2$.*

D.3 Privacy Proof

Theorem 1. *Every UPPRESSO web system for privacy analysis is IdP-private.*

Let $\mathcal{UWS}^{priv}$ be UPPRESSO web system for privacy analysis.

To prove Theorem 1, we have to show that the UPPRESSO web systems $\mathcal{UWS}_1^{priv}$ and $\mathcal{UWS}_2^{priv}$ are indistinguishable. To show the indistinguishability of $\mathcal{UWS}_1^{priv}$ and $\mathcal{UWS}_2^{priv}$, we show that they are indistinguishable under all schedules σ. For this , we first note that for all σ, there is only one run induced by each σ(as our web system, when scheduled, is deterministic). We now proceed to show that for all schedules $\sigma = (\zeta_1, \zeta_2, \dots)$, iff σ induces a run $\sigma(\mathcal{UWS}_1^{priv})$ there exists a run $\sigma(\mathcal{UWS}_2^{priv})$ such that $\sigma(\mathcal{UWS}_1^{priv}) \approx \sigma(\mathcal{UWS}_1^{priv})$

We now show that if two configurations are α-equivalent, then the view of the attacker is statically equivalent.

Lemma 10. *(Same as Lemma 12 in SPRESSO) Let (S_1, E_1, N_1) and (S_2, E_2, N_2) be two α-equivalent configurations. Then $S_1(attacker) \approx S_2(attacker)$.*

Lemma 11. *(Same as Lemma 13 in SPRESSO) The initial configurations (S_1^0, E^0, N^0) of $\mathcal{UWS}_1^{priv}$ and (S_2^0, E^0, N^0) of $\mathcal{UWS}_2^{priv}$ are α-equivalent.*

Proof. Let $\theta = H = L = \emptyset$.Obviously, both latter conditions are true. For all parties $p \in \mathcal{W}_1 \setminus \{b_1\}$, it is clear that $S_1^0(p) = S_2^0(p)$. Also the states $S_1^0(b_1) = S_2^0(b_2)$ are equal. Therefore, all conditions of Definition **??** are fulfilled. Hence, the initial configurations are α-equivalent. □

Lemma 12. *(Same as Lemma 14 in SPRESSO) Let (S_1, E_1, N_1) and (S_2, E_2, N_2) be two α-equivalent configurations of $\mathcal{UWS}_1^{priv}$ and $\mathcal{UWS}_2^{priv}$, respectively. Let $\zeta = \langle ci, cp, \tau_{process}, cmd_{switch}, cmd_{window}, \tau_{script}, url\rangle$ be a web system command. Then, ζ induces a processing step in either both configurations or in none. In the former case, let $(S_1\prime, E_1\prime, N_1\prime)$ and $(S_2\prime, E_2\prime, N_2\prime)$ be configurations induced by ζ such that*

$$(S_1, E_1, N_1) \xrightarrow{\zeta} (S_1\prime, E_1\prime, N_1\prime) and (S_2, E_2, N_2) \xrightarrow{\zeta} (S_2\prime, E_2\prime, N_2\prime) \tag{1}$$

Then $(S_1\prime, E_1\prime, N_1\prime)$ and $(S_2\prime, E_2\prime, N_2\prime)$ are α-equivalent.

Proof. Let θ be a set of proto-tags and H be a set of nonces for which α-equivalence holds and let $L := \bigcup_{a\in\theta} \text{loginSessionTokens}(a, S_1, S_2)$,$K := \{k | \exists n : enc_s(\langle y, n\rangle, k) \in \theta\}$

To induce a processing step, the ci-th message from E_1 or E_2, respectively, is selected.Following Definition 26, we denote these messages by $e_i^{(1)}$ or $e_i^{(2)}$, respectively. We now differentiate between the receivers of the messages by denoting the induced processing steps by

$$\begin{aligned}(S_1, E_1, N_1) &\xrightarrow[p_1 \to E_{out}^{(1)}]{\langle a_1, f_1, m_1\rangle \to p_1} (S_1\prime, E_1\prime, N_1\prime)\\ (S_2, E_2, N_2) &\xrightarrow[p_2 \to E_{out}^{(2)}]{\langle a_2, f_2, m_2\rangle \to p_2} (S_2\prime, E_2\prime, N_2\prime)\end{aligned} \tag{2}$$

Case $p_1 = dns$: In this case, only Cases 1a, 1b and 1c of Definition 80 can apply. Hence, $p_2 = dns$.

(*):As both events are static except for IP addresses, the HTTP nonce, and the HTTPS key, there is no k contained in the input messages(except potentially in tags, from where it cannot be extracted), and the output messages are sent to f_1 or f_2, respectively, they can not cantian any $l \in L$ or $k \in K$. Hence, Condition 2 of Definition 80 holds true.

We note that (*) so-called Condition 2 applies analogously in cases 1a, 1b and 1c. In the case 1a, it is easy to see that $E_{out}^{(1)} \rightleftharpoons_{\theta} E_{out}^{(2)}$.In the case 1c, it is easy to that the DNS server only outputs empty events in both processing steps. In the case 1b, $E_{out}^{(1)}$ and $E_{out}^{(2)}$ are such that Case 1d of Definition 80 applies.

Therefore, $E_1\prime$ and $E_2\prime$ are β-equivalent under (θ, H, L) in all three cases. As there are no changes to any state in all cases, we have that $S_1\prime$ and $S_2\prime$ are γ-equivalent under (θ, H). No new nonces are chosen, hence $N_1\prime = N_1 = N_2 = N_2\prime$.

Case $p_1 = r_1$: In this case, we only distinct several cases of HTTP(S) requests that can happen. The others are ignored the same as SPRESSO.

There are four possible types of HTTP requests that are accepted by r_1 in Algorithm 1:

- path=/script(get the rp-script), Line 3;
- path=/loginSSO(start a login), Line 6;
- path=/startNegotiation(derive a PID_rp), Line 9;
- path=/uploadToken(verify ID token, calculate Acct), Line 18.

From the cases in Definition 26, only two can possibly apply here:Case 1a and Case 1e. For both cases, we will now analyze each of the HTTP requests listed above separately.

Definition 26,Case 1a:$e_i^{(1)} \rightleftharpoons e_i^{(2)}$. This case implies $p_2 = r_1 = p_1$. As we see below, for the output events $E_{out}^{(1)}$ and $E_{out}^{(2)}$ (if any) only Case 1a of Definition 26 applies. This implies the nonce of both the incoming HTTP requests and HTTP responses cannot be in H.

- path=/script In this case, the same output event is produced whose message is
$$\langle HTTPResp, n, 200, \langle\rangle, RPScript\rangle \tag{3}$$
We can note that Condition 5 of Definition 26 holds true and, also, (*) applies.The remaining conditions are trivially fulfilled and $E_1\prime$ and $E_2\prime$ are β-equivalent under (θ, H, L).As there are no changes to any state, we have that $S_1\prime$ and $S_2\prime$ are γ-equivalent under (θ, H). No new nonces are chosen, hence $N_1\prime = N_1 = N_2 = N_2\prime$.
- path=/loginSSO In this case, the reason for equivalence holding is similar to the case above since the same output event is produced.

- path=/startNegotiation(derive a PID_rp), Line 9;
- path=/uploadToken(verify ID token, calculate Acct), Line 18.

□

E Proof of Privacy against RP-based Identity Linkage

E.1 Formal Model of UPPRESSO for Privacy Analysis

Definition 28 (Challenge IdP)**.** *Let dr some domain and $idp(\langle dr_1, dr_2, u\rangle)$ a DY process. We call it a* challenge IdP *iff b is defined exactly the same as a identity server with two exceptions: (1) the state contains one more property, namely challenge, which initially contains the term $\top$. (2) The IdP's algorithm is modified by the following at line 40 in algorithm 2: It is checked if the login request m is addressed to the domain dr_1 If m is addressed to this domain, then the PID_u is generated using the given u. It is also checked if the login request m is addressed to the domain dr_2 and no other message m' was addressed to this domain before (i.e., challenge $\not\equiv \bot$), then the PID_u is generated using the given u and challenge is set to $\bot$ to recorded that a message was addressed to dr_2.*

Definition 29 (UPPRESSO Web System for Privacy Analysis)**.** *Let $\mathcal{UWS} = (\mathcal{W}, \mathcal{S}, \mathsf{script}, E^0)$ be an UPPRESSO web system with $\mathcal{W} = \mathsf{Hon} \cup \mathsf{Web} \cup \mathsf{Net}$, $\mathsf{Hon} = \mathsf{B} \cup \mathsf{RP} \cup \mathsf{IDP}$. (as described in Appendix B.1). $\mathsf{B} = \{b_1, b_2\}$, b_1 is honest and b_2 is malicious and they both own some identities. $\mathsf{RP} = \{r_1, r_2\}$, r_1 and r_2 two (malicious) relying parties, Let $\mathsf{attacker} = \{b_2\} \cup \{r_1, r_2\}$ be some web attacker. Let dr_1 be the domain of r_1, dr_2 be the domain of r_2 and u_{idp} be an identity owned only by IdP, then $idp_c = idp(\langle dr_1, dr_2, u_{idp}\rangle)$ is a challenge IdP. Let $\mathsf{Hon}' := \mathsf{B} \cup \{idp_c\}$, $\mathsf{Web}' := \mathsf{Web}$, and $\mathsf{Net}' := \emptyset$ (i.e., there is no network attacker). Let $\mathcal{W}' := \mathsf{Hon}' \cup \mathsf{Web}' \cup \mathsf{Net}'$. Let $\mathcal{S}' := \mathcal{S} \setminus \{\mathtt{script\_rp}\}$ and script' be accordingly. We call $\mathcal{UWS}^{priv}(dr_1, dr_2, u_{idp}) = (\mathcal{W}', \mathcal{S}', \mathsf{script}', E^0, \mathsf{attacker})$ an* UPPRESSO web system for privacy analysis *iff the domain dr_1 the only domain assigned to r_1, and dr_2 the only domain assigned to r_2. All honest parties (in Hon) are not corruptible, i.e., they ignore any `CORRUPT` message. Relying Parties and some browsers are assumed to be dishonest, and hence, are subsumed by the web attackers.*

References

[1] D. Fett, R. Küsters, and G. Schmitz. Analyzing the browserid sso system with primary identity providers using an expressive model of the web. In *Computer Security–ESORICS 2015: 20th European Symposium on Research in Computer Security, Vienna, Austria, September 21-25, 2015, Proceedings, Part I 20*, pages 43–65. Springer, 2015. C.1, C.1