#7 Thinking in possibilities for federated log out.

Marcel den Reijer & Fouad Makioui

February 7, 2017

Supervised by

Thijs Kinkhorst & Joost van Dijk

Introduction

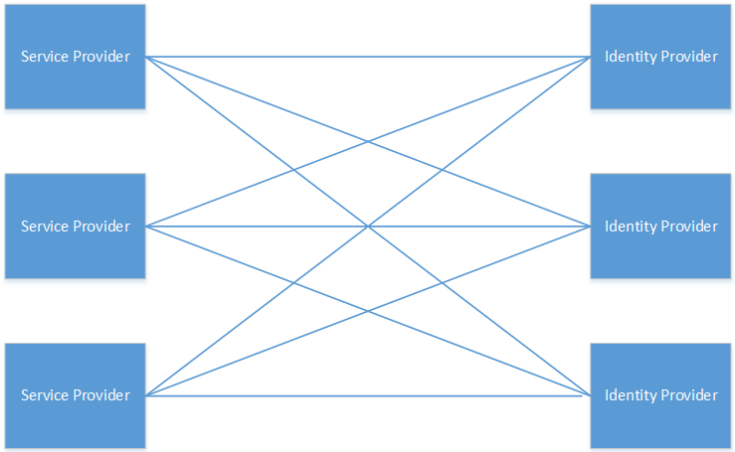
- Authentication & Authorization
- Federated identity
- **SAML 2.0** and OpenID connect
- Logout possibilities

SAML 2.0

- XML based
- Open standard protocol
- Exchange security information
- Parties
  - User Agent
  - Service Provider
  - Identity Provider
- Protocols
  - Single Sign On
  - Single Logout

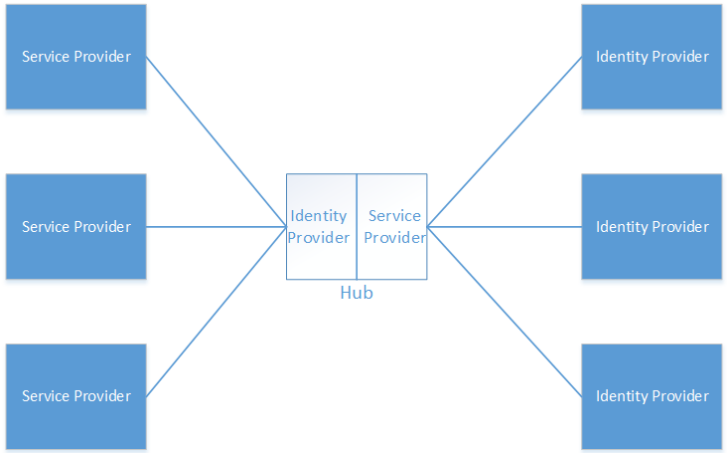
SAML Infrastructures

Mesh



n..n

Hub & Spoke



Service Provider or Identity Provider n..1 Hub

SURFconext (SURFnet)

- Infrastructure for Collaboration
- Based on 99% SAML 2.0 protocol
- 800+ Service Providers
- 173 Identity Providers
- Single Sign On
  - Implemented
- Single Logout
  - Not implemented

SURFconext Infrastructure

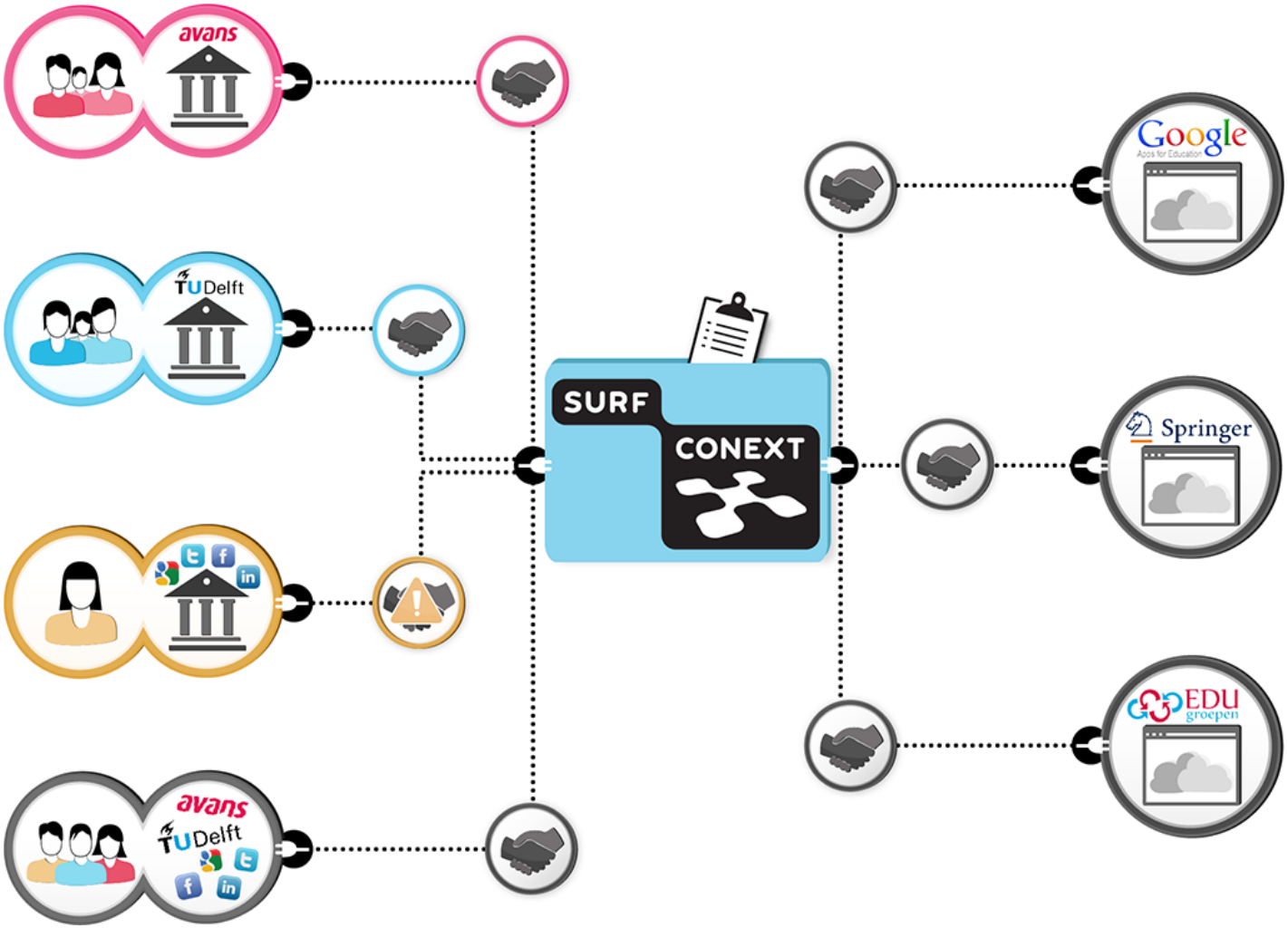


Figure: SURFconext schema [3]

SURFconext Identity Providers

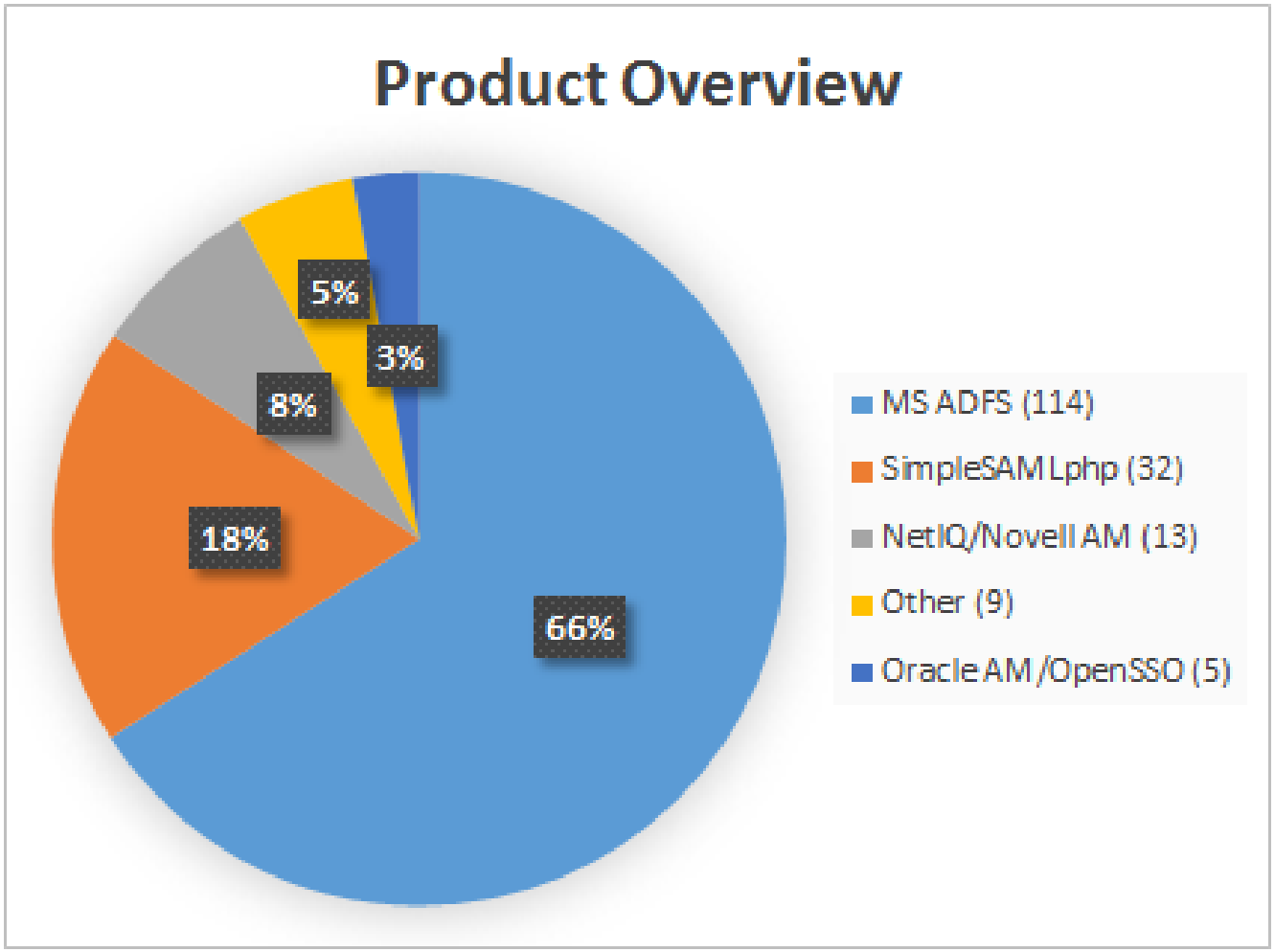


Figure: SURFconext - Identity Providers product overview (13 Jan 2017) [1]

SURFconext Logins

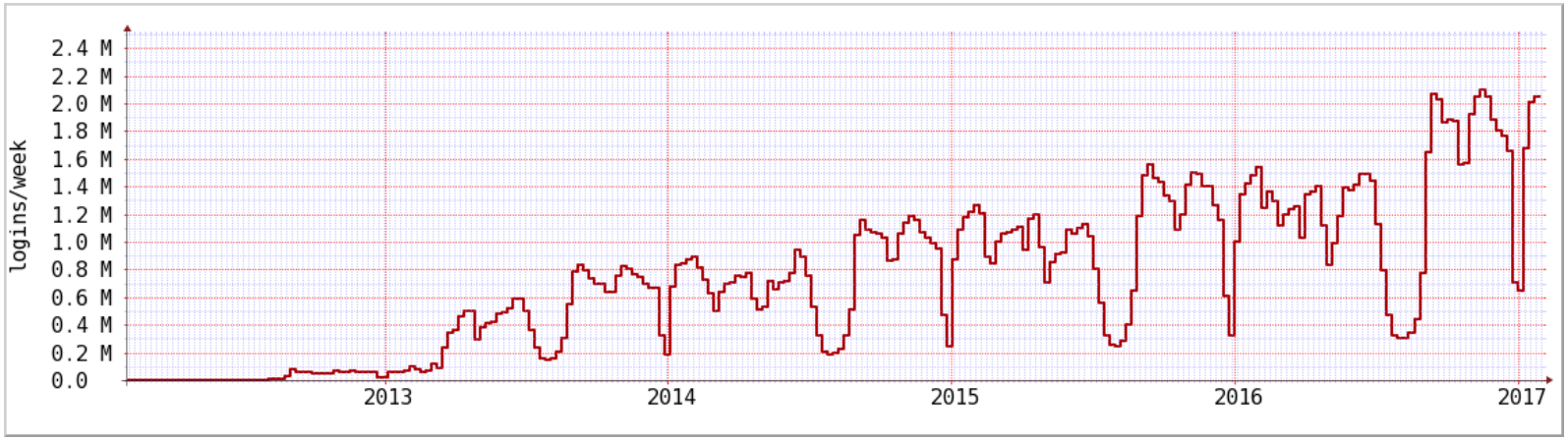


Figure: SURFconext - Login overview (1 Feb 2017)[4]

Research Questions

Based on the introduction we defined the following research question:

- **What are the possibilities for federated log out?**

Sub-questions:

- *What do the users expect to happen when they log out of a service provider?*
- *Based on the user's expectations, which possible solutions provide the user's expectations?*
- *Based on the possible solutions, which is/are the most feasible one(s)?*

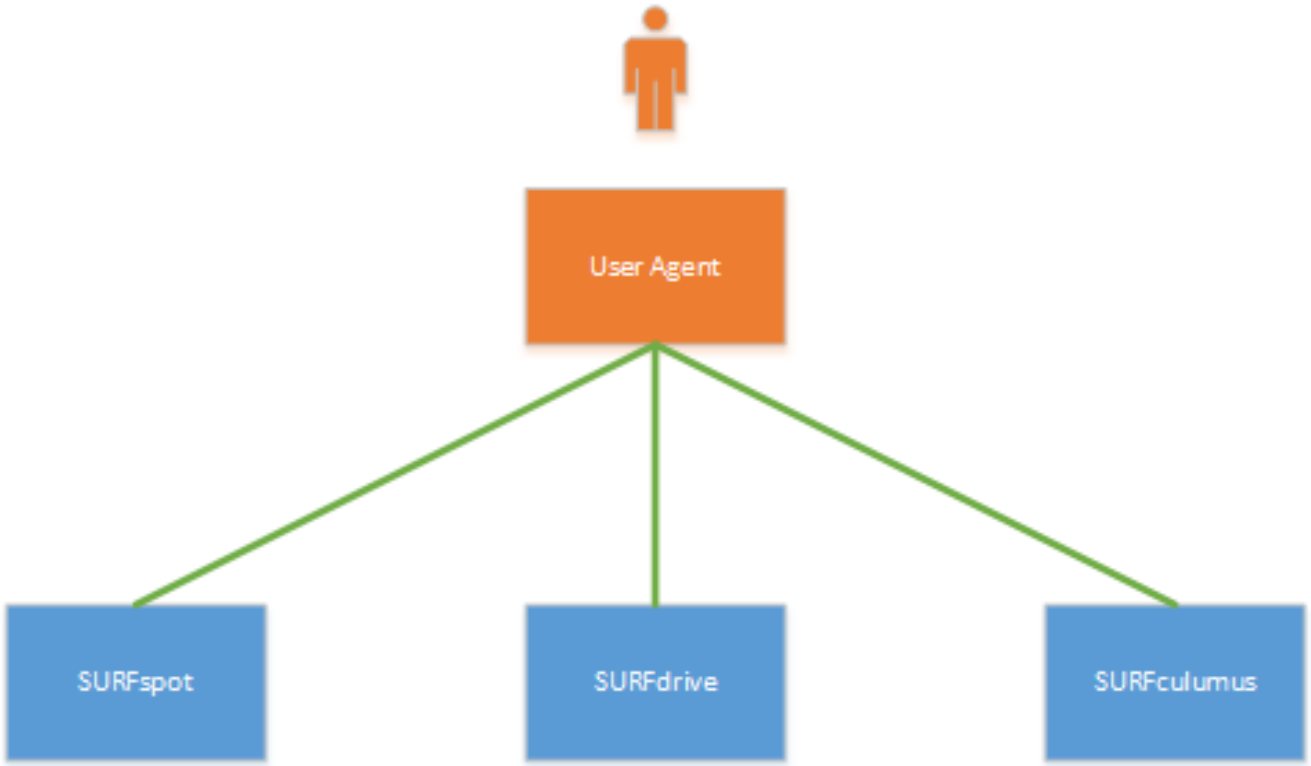
Research

- Interviewing Service Providers
- Desk research
- Possibilities (SURFconext)
- Proof of Concept

Result: Expectation of the users

All Service Providers had the same idea of what the users expect

- Log out by only the application
- Suggestion: Portal overview sessions



Partial Logout

Result: Possible Solutions

- Disabling Single Sign On
- Defining a new protocol in SAML for Partial Logout
- Using the Single Logout protocol for Partial Logout
- ForceAuthn attribute

Possible solution: Disabling Single Sign On

Federation between Service Providers and Identity Provider

- PROS
  - Awareness
  - One Identity
  - Security
- CONS
  - Disproves users usability
  - Inefficient

Possible solution: Defining a new protocol for Partial Logout

Defining a new Protocol

- PROS
  - Flexibility
  - Security
- CONS
  - Design considerations
  - Implementation/Design time
  - Implementation limits (not a Standard)

Possible solution: Using the Single Logout Protocol

Single Logout Protocol
Reason attribute (optional)

- PROS
  - Flexibility SURFconext
  - Standard protocol used by Service Providers
- CONS
  - Service Providers needs to add a attribute
  - SURFconext infrastructure
  - Implementation SURFconext

Possible solution: ForceAuthn attribute

Setting the ForceAuthn in authentication request

- PROS
  - Flexibility Service Providers
  - No additional implementation SURFconext and Identity Providers
  - Standard protocol
- CONS
  - Unambiguously for users
  - Security (current authentication request are not signed)

Suggested solution/Conclusion

- Suggested solution
  - Using the Single Log Out Protocol with additional reason attribute

Working of Single Logout

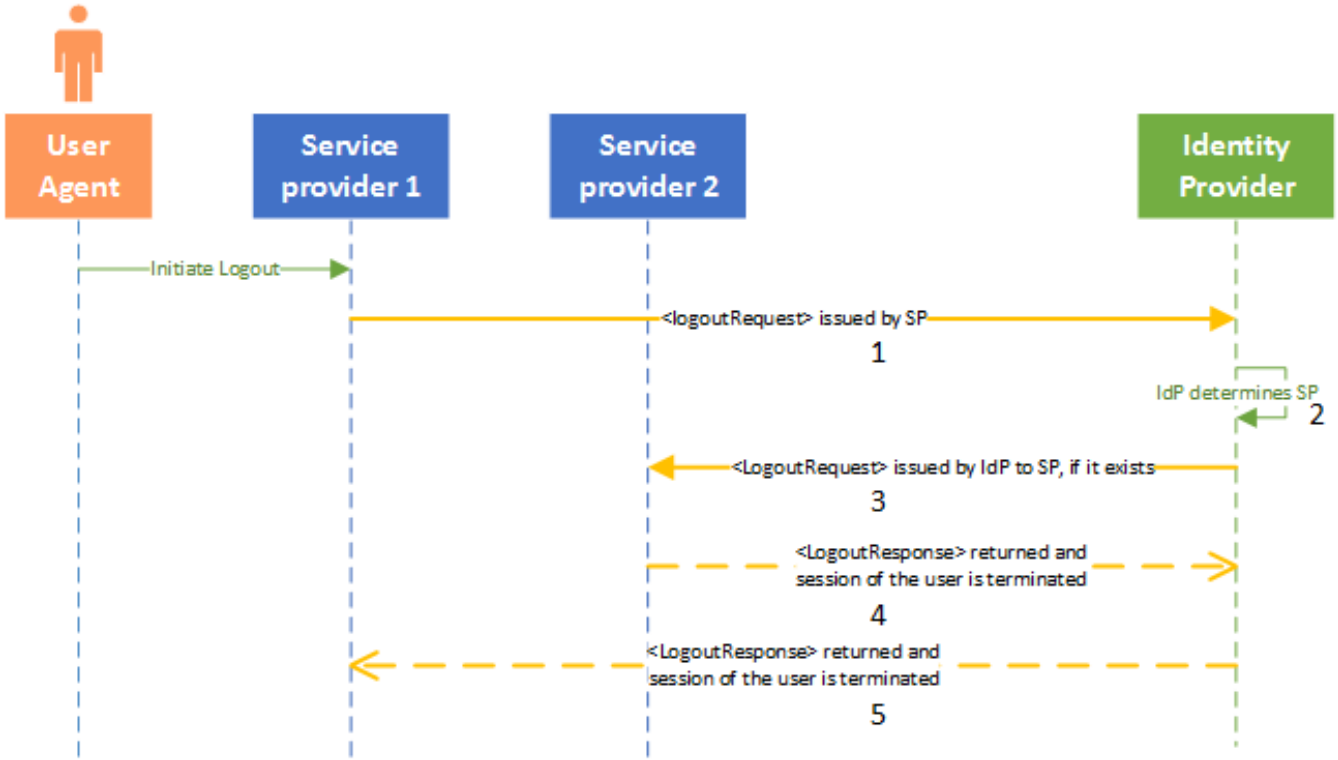


Figure: SAML Single Log Out [2]

Suggested solution

Partial Logout by SURFconext

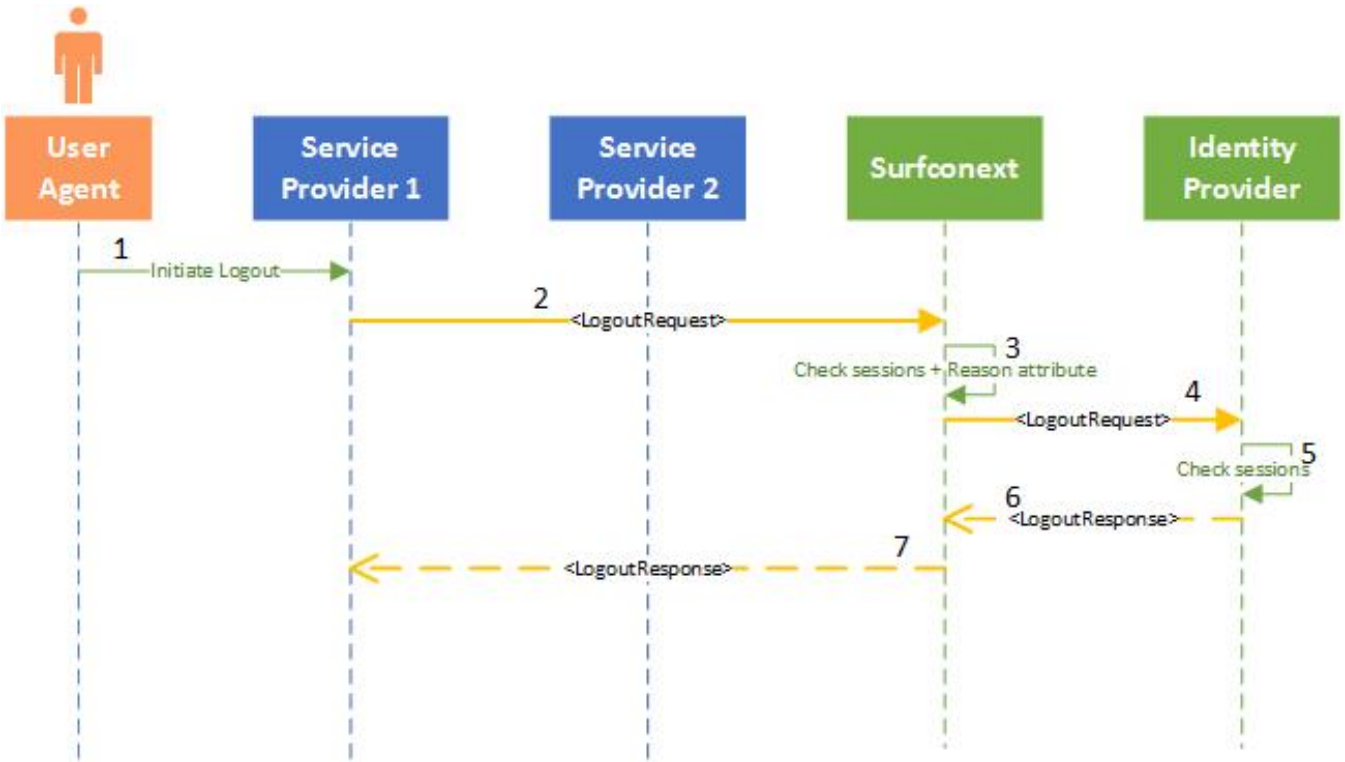


Figure: SAML Partial Logout

Suggested solution

- Log Out Request from Service Provider

```
<samlp:LogoutRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
                     xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                     ID="_4f5f66e61ed4d3c8c51139ce71d35a7507f1e77f9b"
                     Version="2.0"
                     IssueInstant="2017-02-01T18:41:54Z"
                     Destination="https://idp1.example.local/simplesaml/saml2/idp/SingleLogoutService.php"
                     Reason="urn:oasis:names:tc:SAML:2.0:logout:user">
    <saml:Issuer>https://sp2.example.local/simplesaml/module.php/saml/sp/metadata.php/default-sp</saml:Issuer>
    <saml:NameID SPNameQualifier="https://sp2.example.local/simplesaml/module.php/saml/sp/metadata.php/default-sp"
                 Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
                 >_421b6edafdf2e24dd09692821a557746ed99a883ff</saml:NameID>
    <samlp:SessionIndex>_b2eace734b99f1f32bdd57266b8e48a8321a764ea8</samlp:SessionIndex>
</samlp:LogoutRequest>
```

Suggested Feature

Session Overview Portal

- SURFconext records session information
- Specified in the report

Demo

Demo

Thanks... Questions?


Thijs Kinkhorst.
Knowledge surfconext by thijs kinkhorst.
2017.


OASIS.
Saml v2.0 profiles.
2005.


SURFnet.
Documentation of service providers.
2017.


SURFnet.
statistic overview.
2017.