MPI: an authorisation use-case

Mischa Sallé

Nikhef, Amsterdam

27 May 2009

Outline

1. The MPI Use Case
2. Authorisation
   - Shibboleth
   - PKI Certificates
   - Online CA
3. Back to MPI
4. Concluding remarks

Outline

1. The MPI Use Case
2. Authorisation
   - Shibboleth
   - PKI Certificates
   - Online CA
3. Back to MPI
4. Concluding remarks

Outline

1. The MPI Use Case
2. Authorisation
   - Shibboleth
   - PKI Certificates
   - Online CA
3. Back to MPI
4. Concluding remarks

Outline

1. The MPI Use Case
2. Authorisation
   - Shibboleth
   - PKI Certificates
   - Online CA
3. Back to MPI
4. Concluding remarks

- What is MPI?

→ **M**ax **P**lanck **I**nstitute for Psycholinguistics (in Nijmegen)

- They use many "corpora", locally at MPI, also elsewhere

→ Per corpora: access rules

→ *Delegation*: institute A can query institute B *on behalf* of user

MPI

- What is MPI?

→ **M**ax **P**lanck **I**nstitute for Psycholinguistics (in Nijmegen)

- They use many "corpora", locally at MPI, also elsewhere

→ Per corpora: access rules

→ *Delegation*: institute A can query institute B *on behalf* of user

MPI

- What is MPI?

→ **M**ax **P**lanck **I**nstitute for Psycholinguistics (in Nijmegen)

- They use many "corpora", locally at MPI, also elsewhere

→ Per corpora: access rules

→ *Delegation*: institute A can query institute B *on behalf* of user

MPI

- What is MPI?

→ **M**ax **P**lanck **I**nstitute for Psycholinguistics (in Nijmegen)

- They use many "corpora", locally at MPI, also elsewhere

→ Per corpora: access rules

→ *Delegation*: institute A can query institute B *on behalf* of user

- What is MPI?

→ **M**ax **P**lanck **I**nstitute for Psycholinguistics (in Nijmegen)

- They use many "corpora", locally at MPI, also elsewhere

→ Per corpora: access rules

→ *Delegation*: institute A can query institute B *on behalf* of user

Authorisation

- Different systems, e.g.:
  - Shibboleth:
    single-sign-on system, made for webbrowsers, uses SAML statements
  - PKI certificates:
    e.g. Grid world, also webbrowser applications.
    "More complicated".

Authorisation

- Different systems, e.g.:
  - Shibboleth:
    single-sign-on system, made for webbrowsers, uses SAML statements
  - PKI certificates:
    e.g. Grid world, also webbrowser applications.
    "More complicated".

- Different systems, e.g.:
  - Shibboleth:
    single-sign-on system, made for webbrowsers, uses SAML statements
  - PKI certificates:
    e.g. Grid world, also webbrowser applications.
    "More complicated".

Shibboleth (user point of view)

1. User goes to **'service provider'**, e.g. a university library
2. Service provider redirects to **'identity provider'**: typically home institute login page
3. After logging in, the **IdP** redirects back to **SP**, usually with a rewritten URL.
4. The **SP** can see whether user is authorised and for what.

back-channel communication between **SP** and **IdP**

Shibboleth (user point of view)

1. User goes to **'service provider'**, e.g. a university library
2. Service provider redirects to **'identity provider'**: typically home institute login page
3. After logging in, the **IdP** redirects back to **SP**, usually with a rewritten URL.
4. The **SP** can see whether user is authorised and for what.

back-channel communication between **SP** and **IdP**

Shibboleth (user point of view)

1. User goes to **'service provider'**, e.g. a university library
2. Service provider redirects to **'identity provider'**: typically home institute login page
3. After logging in, the **IdP** redirects back to **SP**, usually with a rewritten URL.
4. The **SP** can see whether user is authorised and for what.

back-channel communication between **SP** and **IdP**

Shibboleth (user point of view)

1. User goes to **'service provider'**, e.g. a university library
2. Service provider redirects to **'identity provider'**: typically home institute login page
3. After logging in, the **IdP** redirects back to **SP**, usually with a rewritten URL.
4. The **SP** can see whether user is authorised and for what.

back-channel communication between **SP** and **IdP**

Shibboleth (user point of view)

1. User goes to **'service provider'**, e.g. a university library
2. Service provider redirects to **'identity provider'**:
   typically home institute login page
3. After logging in, the **IdP** redirects back to **SP**, usually with a rewritten URL.
4. The **SP** can see whether user is authorised and for what.

   back-channel communication between **SP** and **IdP**

PKI Certificates (user point of view)

1. User creates a key pair & **C**ertificate **S**igning **R**equest (containing public key)
2. (S)He sends it to **C**ertificate **A**uthority...
3. ... and takes some printed hash of the CSR with passport to **R**egistration **A**uthority to proof he sent the CSR.
4. User receives signed certificate from **CA** and can it use to authenticate.

PKI Certificates (user point of view)

1. User creates a key pair & **C**ertificate **S**igning **R**equest (containing public key)
2. (S)He sends it to **C**ertificate **A**uthority...
3. ... and takes some printed hash of the CSR with passport to **R**egistration **A**uthority to proof he sent the CSR.
4. User receives signed certificate from **CA** and can it use to authenticate.

PKI Certificates (user point of view)

1. User creates a key pair & **C**ertificate **S**igning **R**equest (containing public key)
2. (S)He sends it to **C**ertificate **A**uthority...
3. ... and takes some printed hash of the CSR with passport to **R**egistration **A**uthority to proof he sent the CSR.
4. User receives signed certificate from **CA** and can it use to authenticate.

PKI Certificates (user point of view)

1. User creates a key pair & **C**ertificate **S**igning **R**equest (containing public key)
2. (S)He sends it to **C**ertificate **A**uthority...
3. ... and takes some printed hash of the CSR with passport to **R**egistration **A**uthority to proof he sent the CSR.
4. User receives signed certificate from **CA** and can it use to authenticate.

Combining the two...

- Use an online CA:

  produce certificates without human intervention

- Online CA is a Shibboleth SP

→ service is the *production of certificates*

→ Shibboleth IdP plays the role of RA, to check the user identity (username/password ↔ passport).

→ short-lived ($\lesssim 10^6 \mathrm{sec}$) credential service (SLCS)

- Much easier for the user: only standard username/password.

Combining the two...

- Use an online CA:

  produce certificates without human intervention

- Online CA is a Shibboleth SP

→ service is the *production of certificates*

→ Shibboleth IdP plays the role of RA, to check the user identity (username/password ↔ passport).

→ short-lived ($\lesssim 10^6 \mathrm{sec}$) credential service (SLCS)

- Much easier for the user: only standard username/password.

Combining the two...

- Use an online CA:

  produce certificates without human intervention

- Online CA is a Shibboleth SP

$\longrightarrow$ service is the *production of certificates*

$\longrightarrow$ Shibboleth IdP plays the role of RA, to check the user identity (username/password $\leftrightarrow$ passport).

$\longrightarrow$ short-lived ($\lesssim 10^6 \mathrm{sec}$) credential service (SLCS)

- Much easier for the user: only standard username/password.

Combining the two...

- Use an online CA:

  produce certificates without human intervention

- Online CA is a Shibboleth SP

$\longrightarrow$ service is the *production of certificates*

$\longrightarrow$ Shibboleth IdP plays the role of RA, to check the user identity (username/password $\leftrightarrow$ passport).

$\longrightarrow$ short-lived ($\lesssim 10^6 \mathrm{sec}$) credential service (SLCS)

- Much easier for the user: only standard username/password.

Combining the two...

- Use an online CA:

  produce certificates without human intervention

- Online CA is a Shibboleth SP

$\longrightarrow$ service is the *production of certificates*

$\longrightarrow$ Shibboleth IdP plays the role of RA, to check the user identity (username/password $\leftrightarrow$ passport).

$\longrightarrow$ short-lived ($\lesssim 10^6 \mathrm{sec}$) credential service (SLCS)

- Much easier for the user: only standard username/password.

Combining the two...

- Use an online CA:

  produce certificates without human intervention

- Online CA is a Shibboleth SP

$\longrightarrow$ service is the *production of certificates*

$\longrightarrow$ Shibboleth IdP plays the role of RA, to check the user identity (username/password $\leftrightarrow$ passport).

$\longrightarrow$ short-lived ($\lesssim 10^6 \mathrm{sec}$) credential service (SLCS)

- Much easier for the user: only standard username/password.

SLCS (cont.)

1. User browses to online CA
2. Gets redirected to IdP (home institution login)
3. After login redirected back to online CA
4. (S)He or browser sends in CSR
5. User receives signed certificate

SLCS (cont.)

1. User browses to online CA
2. Gets redirected to IdP (home institution login)
3. After login redirected back to online CA
4. (S)He or browser sends in CSR
5. User receives signed certificate

SLCS (cont.)

1. User browses to online CA
2. Gets redirected to IdP (home institution login)
3. After login redirected back to online CA
4. (S)He or browser sends in CSR
5. User receives signed certificate

SLCS (cont.)

1. User browses to online CA
2. Gets redirected to IdP (home institution login)
3. After login redirected back to online CA
4. (S)He or browser sends in CSR
5. User receives signed certificate

SLCS (cont.)

1. User browses to online CA
2. Gets redirected to IdP (home institution login)
3. After login redirected back to online CA
4. (S)He or browser sends in CSR
5. User receives signed certificate

Back to MPI

- MPI uses a java browser (standalone tool) → *complication*
- Certificates will be fully hidden from the user...
- ...but can be used for delegation
- Also: will use one-time certificates:
  user cannot loose key, certificate etc.

Back to MPI

- MPI uses a java browser (standalone tool) $\longrightarrow$ *complication*
- Certificates will be fully hidden from the user...
- ...but can be used for delegation
- Also: will use one-time certificates:
  user cannot loose key, certificate etc.

Back to MPI

- MPI uses a java browser (standalone tool) → *complication*
- Certificates will be fully hidden from the user...
- ...but can be used for delegation
- Also: will use one-time certificates:
  user cannot loose key, certificate etc.

Back to MPI

- MPI uses a java browser (standalone tool) $\longrightarrow$ *complication*
- Certificates will be fully hidden from the user...
- ...but can be used for delegation
- Also: will use one-time certificates:
  user cannot loose key, certificate etc.

Concluding remarks

- Status
  - SURFnet is running online CA (testphase)
  - MPI and SURFnet have IdP, part of SURFnet Federation (production)
  - MPI is adapting its service providers: certificates with Shibboleth as fallback (complications)
  - Nikhef (me) is doing client site: adapting the java tool (testphase)
- Other projects:
  - SWITCH → Grid SLCS service
  - Nordic → now almost European (SL)CS service, also incl. SURFnet & Terena

Concluding remarks

- Status
  - SURFnet is running online CA (testphase)
  - MPI and SURFnet have IdP, part of SURFnet Federation (production)
  - MPI is adapting its service providers: certificates with Shibboleth as fallback (complications)
  - Nikhef (me) is doing client site: adapting the java tool (testphase)
- Other projects:
  - SWITCH → Grid SLCS service
  - Nordic → now almost European (SL)CS service, also incl. SURFnet & Terena

Concluding remarks

- Status
  - SURFnet is running online CA (testphase)
  - MPI and SURFnet have IdP, part of SURFnet Federation (production)
  - MPI is adapting its service providers: certificates with Shibboleth as fallback (complications)
  - Nikhef (me) is doing client site: adapting the java tool (testphase)
- Other projects:
  - SWITCH → Grid SLCS service
  - Nordic → now almost European (SL)CS service, also incl. SURFnet & Terena

Concluding remarks

- Status
  - SURFnet is running online CA (testphase)
  - MPI and SURFnet have IdP, part of SURFnet Federation (production)
  - MPI is adapting its service providers: certificates with Shibboleth as fallback (complications)
  - Nikhef (me) is doing client site: adapting the java tool (testphase)
- Other projects:
  - SWITCH → Grid SLCS service
  - Nordic → now almost European (SL)CS service, also incl. SURFnet & Terena

Concluding remarks

- Status
  - SURFnet is running online CA (testphase)
  - MPI and SURFnet have IdP, part of SURFnet Federation (production)
  - MPI is adapting its service providers: certificates with Shibboleth as fallback (complications)
  - Nikhef (me) is doing client site: adapting the java tool (testphase)
- Other projects:
  - SWITCH → Grid SLCS service
  - Nordic → now almost European (SL)CS service, also incl. SURFnet & Terena

Concluding remarks

- Status
  - SURFnet is running online CA (testphase)
  - MPI and SURFnet have IdP, part of SURFnet Federation (production)
  - MPI is adapting its service providers: certificates with Shibboleth as fallback (complications)
  - Nikhef (me) is doing client site: adapting the java tool (testphase)
- Other projects:
  - SWITCH → Grid SLCS service
  - Nordic → now almost European (SL)CS service, also incl. SURFnet & Terena

Concluding remarks

- Status
  - SURFnet is running online CA (testphase)
  - MPI and SURFnet have IdP, part of SURFnet Federation (production)
  - MPI is adapting its service providers: certificates with Shibboleth as fallback (complications)
  - Nikhef (me) is doing client site: adapting the java tool (testphase)
- Other projects:
  - SWITCH → Grid SLCS service
  - Nordic → now almost European (SL)CS service, also incl. SURFnet & Terena

Concluding remarks

- Status
  - SURFnet is running online CA (testphase)
  - MPI and SURFnet have IdP, part of SURFnet Federation (production)
  - MPI is adapting its service providers: certificates with Shibboleth as fallback (complications)
  - Nikhef (me) is doing client site: adapting the java tool (testphase)
- Other projects:
  - SWITCH $\rightarrow$ Grid SLCS service
  - Nordic $\rightarrow$ now almost European (SL)CS service, also incl. SURFnet & Terena

SWITCH Model - SLCS