Anonymous Credentials in Web Applications

A Child’s Play with the PRIME Core

Benjamin.Kellermann@tu-dresden.de
D19E 04A8 8895 020A 8DF6
0092 3501 1A32 491A 3D9C

Immanuel.Scholz@tu-dresden.de
EC9D D587 BDF0 0199 CE39
37B8 FFAE CFEF 5707 11EA

Nice, September 10, 2009
Possible Example Applications

Wolfenstein 3D

*Wolfenstein 3D* (originally *Wolfens*) popularized the first-person shooter genre on May 5, 1992 for MS-DOS.

**Contents**

1. Plot
2. Cheat codes
   - 2.1 Customer Cheat
   - 2.2 Debug Mode
   - 2.3 Jukebox
   - 2.4 Tech Support Command Line

**Additional Applications**

- [yourhomework.com](http://yourhomework.com)
- [Safebook](http://safebook.com)
- [DiagnoseMe.com/Forum](http://diagnoseme.com/forum)
Possible Example Applications

- Facebook
- Wiki4Games

Children Under Age 13

Facebook does not knowingly collect or solicit personal information from anyone under the age of 13 or knowingly allow such persons to register. If you are under 13, please do not attempt to register for Facebook or send any information about yourself to us, including your name, address, telephone number, or email address. No one under age 13 may provide any personal information to or on Facebook. In the event that we learn that we have collected personal information from a child under age 13 without verification of parental consent, we will delete that information as quickly as possible. If you believe that we might have any information from or about a child under 13, please contact us through the form on our privacy help page.

Children Between the Ages of 13 and 18

We recommend that minors 13 years of age or older ask their parents for permission before sending any information about themselves to anyone over the Internet.
Naive Implementation
Naive Implementation
Solution

problems, requirements
Solution

problems, requirements

idemix

Benjamin Kellermann
Anonymous Credentials in Web Applications
Solution

problems, requirements

Benjamin Kellermann
Anonymous Credentials in Web Applications
slide 4 of 10
Solution

problems, requirements

SOLVED

???
Problem
Comparison – PGP
Comparison – PGP
Comparison – PGP

GnuPG

PGP
Prime Architecture

Firefox
1: user enters Web page

2: access Web page

Application
Prime Architecture

1: user enters Web page
2: access Web page

Firefox
Application

client PRIME core
server PRIME core

123
Prime Architecture

1: user enters Web page

2: access Web page

3: ask PRIME

4: ask PRIME

5: ask PRIME

6: show credentials
Prime Architecture

1: user enters Web page
2: access Web page
3: ask PRIME
4: ask PRIME

client PRIME core

Firefox

Application

server PRIME core
Prime Architecture

1: user enters Web page
2: access Web page
3: ask PRIME
4: ask PRIME
5: ask User

Firefox
Interceptor
client PRIME core

Application
server PRIME core
Prime Architecture

1: user enters Web page
2: access Web page
3: ask PRIME
4: ask PRIME
5: ask User
6: show credentials

client core

server core

Firefox

Interceptor

Application
Demo

Live Demonstration
Warning, Bugs around
Conclusion

- Developers need easy Toolkit
- 10 lines of additional code for anonymous credentials!
- easy to use interface
- good tutorial documentation
- easy to set up issuing service
Thank you for your attention!

Discussion

Benjamin.Kellermann@tu-dresden.de
D19E 04A8 8895 020A 8DF6
0092 3501 1A32 491A 3D9C

Immanuel.Scholz@tu-dresden.de
EC9D D587 BDF0 0199 CE39
37B8 FFAE CFEF 5707 11EA

Nice, September 10, 2009