

INCORPORATING X.509 SECURITY CERTIFICATE BASED AUTHENTICATION INTO SHIBBOLETH AUTHENTICATION MECHANISM

Veerendra Shirole¹ and Gordon K Springer^{1,2}

**Computer Science Department¹ & MU
Informatics Institute²**

University of Missouri

OUTLINE

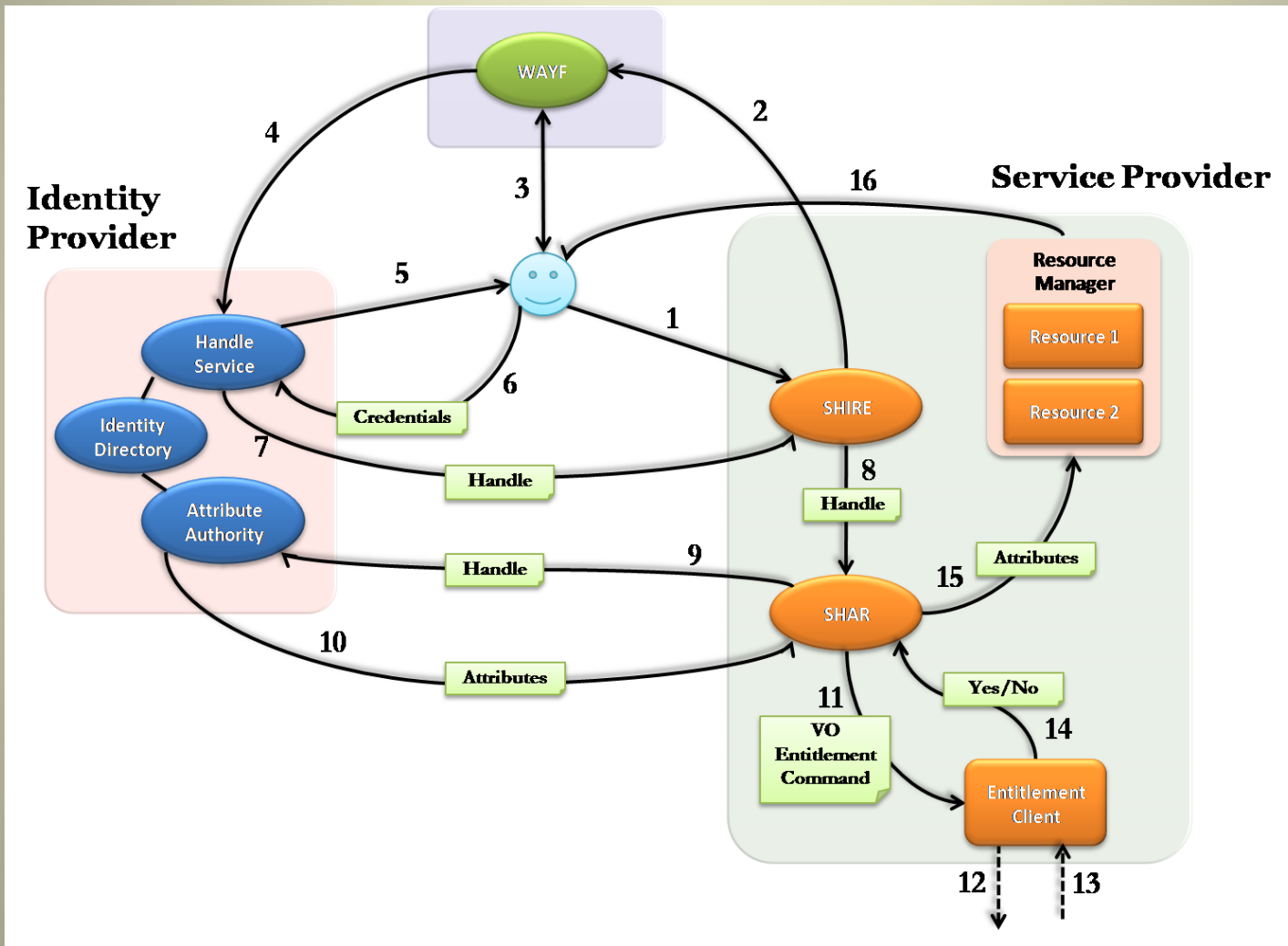
- ◉ Introduction to Shibboleth Authentication
- ◉ Limitations
- ◉ Objective of this project
- ◉ Methodology
- ◉ Advantages of Certificate Based Authentication
- ◉ Conclusion
- ◉ Questions & Answers

INTRODUCTION

- ◎ GPN is a federation of research universities providing access to computing resources
- ◎ Distributed Authentication & Authorization managed using Shibboleth

INTRODUCTION

SHIBBOLETH AUTHENTICATION



LIMITATIONS

- ⦿ Authentic users without Shibboleth credentials cannot get access to resources

- ⦿ Current solution is to provide the users with credentials for one of the Shibboleth Identity Providers

OBJECTIVE

- ◎ Authenticate users that are not affiliated to an institution or do not have Shibboleth credentials but are entitled to use the resources
- ◎ Provide an additional method of authentication using X.509 certificates
- ◎ Entitlements need to be maintained for authorization decisions

METHODOLOGY



ADVANCING RESEARCH | CREATING SOLUTIONS

[About GPN](#) : [FAQ](#) : [Help](#) : [Privacy](#)

Select your Home Organisation

In order to access a Resource on host 'osprey.rnet.missouri.edu' you must authenticate yourself.

OR

Provide a Security Certificate

Remember selection for this web browser session.

> The [SWITCH](#) Foundation operates the Swiss Education & Research Network which guarantees high-speed connectivity to the Internet and to science networks globally for the benefit of higher education in Switzerland.

SAMPLE OUTPUT

```
[vshirole@nighthawk ~/doegrids]$ ./TestCert usercert.pem
```

Distinguished Name: Veerendra Shirole

Email Address:

Certificate Issued By: Globus Simple CA

error 20 at 0 depth lookup:unable to get local issuer certificate

```
[vshirole@nighthawk ~/doegrids]$ ./TestCert springer.pk12
```

Distinguished Name: Gordon K Springer 310002

Email Address: springer@cs.missouri.edu

Certificate Issued By: DOEGrids CA 1

error 10 at 0 depth lookup:certificate has expired

```
[vshirole@nighthawk ~/doegrids]$ ./TestCert Test-100204.pem
```

Distinguished Name: Gordon K Springer 790192

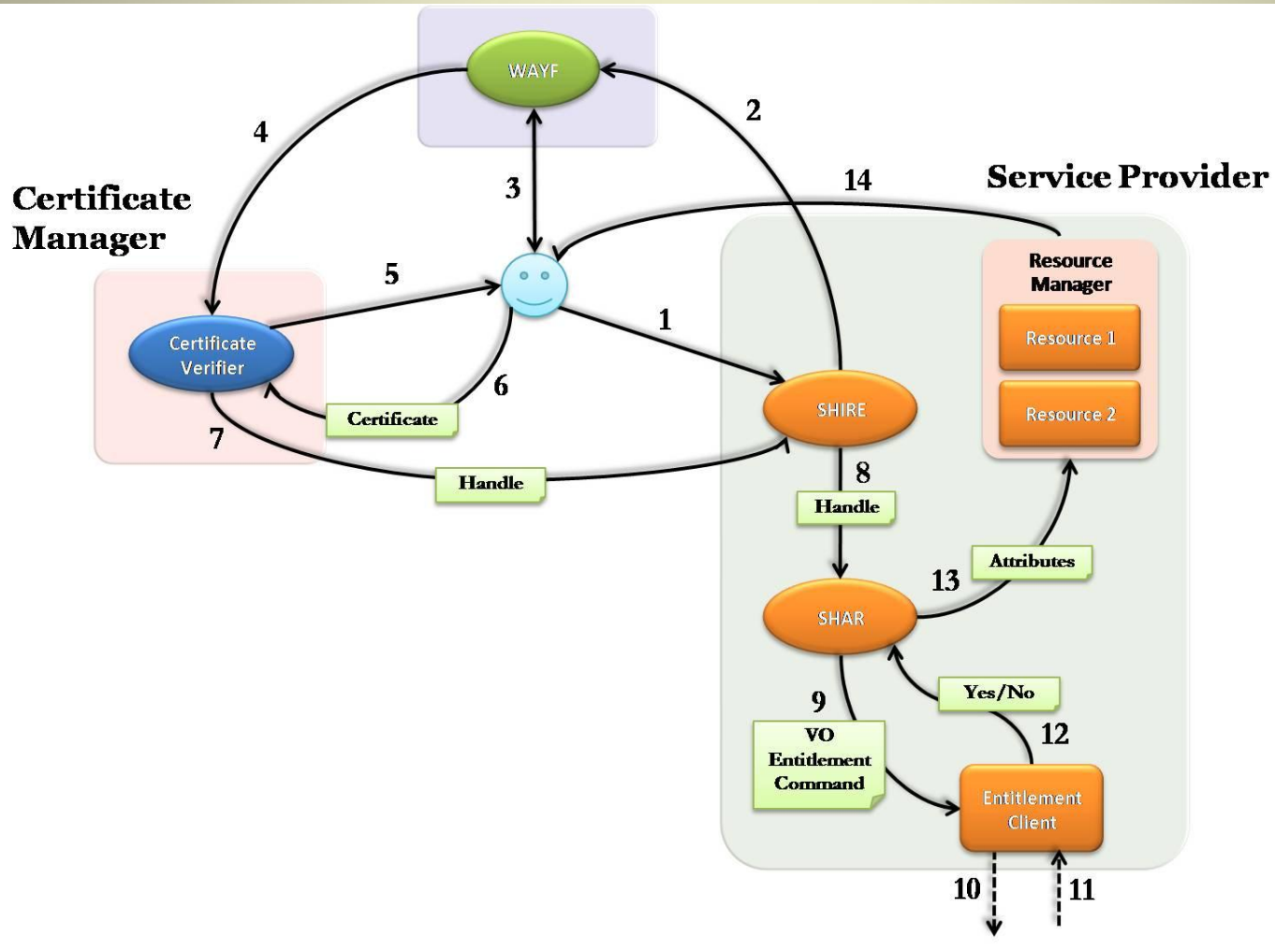
Email Address: springer@cs.missouri.edu

Certificate Issued By: DOEGrids CA 1

The Certificate is Valid!

METHODOLOGY

Alternate Flow: X.509 certificate



ADVANTAGES

- ◉ An additional measure for user authentication
- ◉ Validity of a security certificate can be controlled
- ◉ Recognized Certificate Authorities can be controlled
- ◉ Returning users only need a new certificate

CONCLUSION

- Provides the capability of accepting security certificates as an alternative for verifying user identity
- Authentic users with no Shibboleth credentials can access resources provided by GPN
- Minimal changes to the existing authentication architecture and no changes to the authorization mechanism

THANK YOU



QUESTIONS ?