EUROPEAN MIDDLEWARE INITIATIVE

EMI SECURITY ARCHITECTURE

ASSESSMENT AND FUTURE DIRECTIONS

Document identifier:	
Date:	**15/12/2012**
Activity:	**JRA1 –**
Lead Partner:	**UH**
Document status:	**Draft**
Document link:	

Abstract:
This document provides a description of the EMI security framework architecture and an assessment of its strengths and potential weaknesses. A set of recommendations and directions for future work are provided.

I. DELIVERY SLIP

	Name	Partner/Activity	Date
From	John White	UH/JRA1	
Reviewed by			
Approved by			

II. DOCUMENT LOG

Issue	Date	Comment	Author/Partner

III. DOCUMENT CHANGE RECORD

Issue	Item	Reason for Change

IV. DOCUMENT AMENDMENT PROCEDURE

This document can be amended by the JRA1 Security Area task leader or people appointed by him/her to this task further to any feedback from other teams or people. Minor changes, such as spelling corrections, content formatting or minor text re-organization not affecting the content and meaning of the document can be applied by the task leader without peer review. Other changes must be submitted to peer review and to the EMI PEB and TCB for approval.

When the document is modified for any reason, its version number shall be incremented accordingly. The document version number shall follow the standard EMI conventions for document versioning. The document shall be maintained in the CERN CDS repository and be made accessible through the OpenAIRE portal.

V. GLOSSARY

VI. COPYRIGHT NOTICE

TABLE OF CONTENTS

1 INTRODUCTION

1.1 EXECUTIVE SUMMARY

[A brief summary of the content of the document. It must give the reader an idea of what is described and the main points of each chapter in a condensed way]

1.2 DOCUMENT ORGANISATION

[A description of the document organization by chapter]

2 OVERVIEW OF THE EMI SECURITY ARCHITECTURE

2.1 DEFINITION OF SECURITY ARCHITECTURE

[Definition of security architecture or framework in general and in the context of distributed grid computing, basic principles]

2.2 TRUST, AUTHENTICATION AND AUTHORIZATION: A TERMINOLOGY

[Definitions of the most important concepts]

2.3 VIRTUAL ORGANIZATION, SITES AND COMMON GRID SERVICES

[Definitions, brief description of the major grid services and how security applies to them]

2.4 AUTHENTICATION

2.4.1 Identity Credential Formats

2.4.2 Short-Lived Credential Services

2.4.3 Bootstrapping Authentication

2.4.4 Enforcing Validity Constraints

2.4.5 Revocation

2.4.6 Certificate Renewal

2.4.7 Delegation

2.4.8 Renewal of Proxy Certificates

2.4.9 Anonimity, Privacy, Pseudonimity

2.4.10 EMI Common Services and Libraries

2.4.10.1 CAnL

2.4.11 ARC, gLite and UNICORE Security Services

2.4.11.1 VOMS, UVOS, etc.

2.5 USER KEY MANAGEMENT

2.5.1 Hydra

2.6 AUTHORISATION

2.6.1 Policy Definition and Management

2.6.2 Argus

2.7 IDENTITY SWITCHING

2.7.1 glExec

2.8 DATA MANAGEMENT, ENCRYPTION, CONFIDENTIALITY

2.9 FEDERATED IDENTITIES

2.9.1 STS

2.10 LOGGING, TRACING, AUDITING

2.11 SECURITY MANAGEMENT AND THREATS HANDLING

2.11.1 Software Security Management

2.11.1.1 Bug fixing, Emergency Releases, etc.

2.11.2 Grid Services Security Assessment

2.11.3 Security Response Teams and Coordination Bodies

2.11.4 International Collaborations

2.11.4.1 OGF, IGTF, etc

2.12 ASSESSMENT, STRENGTHS, AREAS FOR IMPROVEMENT