MSSP Metadata – Fact sheet

v1.0

Introduction

ETSI MCOMM standards based mobile signature service consists of mobile signature service providers (MSSP) and application providers (AP). MSSP entities have different roles such as Acquiring Entity, Routing Entity, Identity Issuer and Home MSSP. Connected MSSPs constitute a mobile signature service system known as a Mesh. The Mesh has been defined in the ETSI TS 102 207 standard (figure 1). This is also known as a mobile signature roaming.

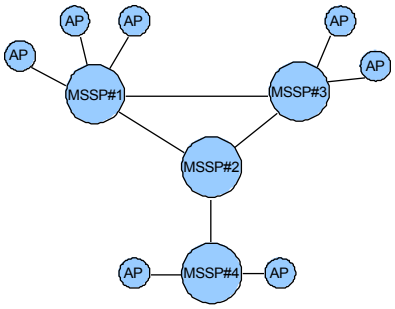

Figure 1. Multiple MSSPs constitute a Mesh.

Security of the mobile signature roaming is based on shared communication addresses, mutual TLS authentication of the entities and a message integrity based on XML signatures. This trust model relies on X509 certificates. These certificates must be shared between entities in a secure way and a life cycle of these certificates needs to be taken care of. We need a way describing and managing this information in a commonly interpreted and secure way.

MSSP metadata

The MSSP metadata defines an XML file that contains mobile signature system entities and the security and communication parameters between these entities. By publishing MSSP metadata MSSPs not only extend the Mesh security but also make it easier to manage. The MSSP metadata replaces ETSI TS 102 204 standard MSS HandshakeService method in a secure way.

The base or reference model for this metadata is the Metadata for the OASIS Security Assertion Markup Language V2.0 (SAML2). If you are familiar with the SAML2 metadata, you should find that fundaments of MSSP metadata have been organized in the same way.

The MSSP metadata defines XML signature and TLS/SSL metadata among system entities. The MSSP metadata also introduces XML encryption metadata support for mobile signature services. XML encryption can be used especially by a mobile signature registration method when distributing confidential data over the Internet.

MSSP Metadata Content

MSSP metadata is organized under a top level EntitiesDescriptor element which contains a collection of sub level EntitiesDescriptor elements and EntityDescriptor elements. EntityDescriptor is defined for each MSSP and AP. EntityDescriptor defines further an entity's services, capabilities and public key certificates. EntityDescriptors may be gathered into a new EntitiesDescriptor container element. The EntitiesDescriptor is the primary unit of MSSP metadata (figure 2).

Sub level EntitiesDescriptor can be used in large MSSP networks to manage separate mobile signature subnets. For example each mobile operator may have their own EntitiesDescriptor that contains only one operator's Verifying Entities, Home MSSPs, APs etc.
Public MSSP metadata is generally needed when establishing large interconnected Mesh on national level.

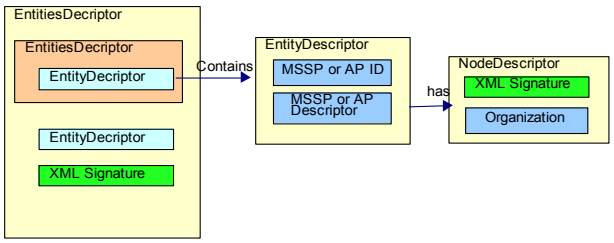

Figure 2. EntitiesDescriptor's content.

MSSP metadata blocks can be digitally signed and verified. The mechanisms help in establishing trust in the accuracy and authenticity of MSSP metadata.

Kiuru MSSP metadata support

Kiuru MSSP server trust management is based on MSSP metadata v1.0 draft. Each Kiuru MSSP server is able to generate it's own metadata.xml file and you can manage SSL, XML signatures and XML encryption easily by exchanging/publishing these metadata files.

Kiuru MSSP manages the life cycle of all certificates. You can have multiple valid certificates in place at the same time. Therefore you may take in use a new certificate and use an aging one simultaneously. There is no need for multi-party synchronous updates.

About Methics

Methics Ltd is a privately held ISV, which has developed PKI and wireless PKI products for application providers and operators and built unique security and performance testing tools for operators. For more information, call us at

tel. +358 (0)9 5840 0188
e-mail methics.sales@methics.fi