Token-based Payment in Dynamic SAML-based Federations

David J. Lutz[1] and Burkhard Stiller[2]

[1] Rechenzentrum Universitaet Stuttgart
Allmandring 30; 70550 Stuttgart; Germany
David.Lutz@rus.uni-stuttgart.de
[2] University of Zurich, Department of Informatics (IFI)
Binzmühlestr. 14, CH-8050 Zürich, Switzerland
stiller@ifi.uzh.ch

Abstract. The newly developed approach on token-based payments introduces an integration of payments with current schemes for Identity Federations based on SAML. This new design utilizes an established federation infrastructure as well as its protocols. Only relevant mechanisms to support the payment on the federation infrastructure level are extended.

Keywords: Payment Token, Payment Assertion, Identity Federation, Payment

1 Introduction

The concept of Identity Federation is quite well known and understood in the academic [8] as well as in the business area [4]. Within such a federation, several service providers agree on accepting user authentication not at their systems, but on the user's home institution, e.g., the user's universtity or his/her telecom operator. This leads to a reduced efford regarding the administration of credentials on both the user's side (only one account at the idenity provider and not several at each service provider) and the service provider's side (only simple account management needed). Almost all of these federations focus on authentication and authorization[3], an essential aspect is missing today: payment. Currently, payment is build on top of the federation structure using specific payment protocols, which means additional work and security concerns for the implementation itself. It is quite obvious that an implementation of payment solutions on the federation level would allow for an easy setup of business federations without considering payment solutions separately. Therefore, this work, partly developed in the SWIFT [7] project, focuses on the development of a payment scheme for identity federations without touching the federation structure itself to allow for an easy use of payment structures without the need of rebuilding the federation.

[3] For both purposes mainly the Security Assertion Markup Language (SAML) is used.

This means that the former high-level payment could now be done by using the federation language (SAML [2], XACML [6]), its protocols (e.g., HTTP, SOAP) and its structure (service provider, identity provider, user), whereas the original federation concept should be kept unchanged as far as possible.

2 Related Work

Since the token-based payment approach builds on Identity Federations and the payment for electronic business, this section briefly introduces Identity Federations and discusses possible electronic payment mechanisms.

Many different Identity Federation approaches have been developed over the last years, like CAS, PERMIS, VOMS, all related to the Grid area, and Shibboleth [8], Liberty Alliance [4] and Web Service Federation [5] from within the web community. The key concept of such an Identity Federation is the Single Sign-on (SSO) principle, which means that a user has to log in only once. To do so, the user's profile is stored at a component called Identity Provider (IdP). Whenever a user wants to access a service, he authenticates himself at his IdP and receives after a successfully login an assertion or a token that is used as an identifier inside this federation. If a user requests a service at a Service Provider (SP), he presents the token/assertion from the IdP to claim his identity. Since all IdPs and SPs in such a federation have a contractually established trust relationship, the SP can trust the token/assertion based on the IdP's signature. If the SP needs specific user attributes, he requests them directly from the user's IdP, which releases them based on the release policy the user has chosen. Afterwards, the SP evaluates submitted attributes to decide on the access.

In electronic commerce, three different schemes of handling electronic payments exist: the transmission of payment-related information, the transmission of exchange information, and the transmission of digital cash. Although the implementation of the two firstly mentioned approaches in a federation infrastructure would also show some improvement regarding the convenience of payment, our work applies the third scheme. The transmitted information can be used as cash within the federation. Early approaches like NetCash and Digital Cash [1] covered ideas that a piece of information may be interpreted and used like money. These ideas of digital cash determine the foundation for the payment-enabled Identity Federation.

3 Payment-enabled Identity Federation

The key idea of this work is to enable a payment within an Identity Federation and without changing the federation's infrastructure, protocols, or languages. Since most important federations today are based on SAML and an architecture including an Identity Provider, a Service Provider, and the User, it is straightforward that the new payment-enabled federation is also based on SAML and supports this common infrastructure.

The concept of the **Identity Provider** (IdP) does not have to be changed compared to its functions in usual SAML-based federations. It authenticates the user based on contracts as well as credentials and sends after a successfully login a token or assertion for further authentication to the consumer. It also sends attribute information for authorization purposes to the Service Provider.

The **Service Provider** (SP) has to be extended, because it needs the possibility to use additional hardware and software. Besides this, policy decision functions have to be changed in a way that a request for payment is sent to the user and upon the reception of a valid payment it has to be evaluated.

The **Payment Provider** (PP) determines the new component that enables the payment within an Identity Federation. It hosts the user's account, thus, it may become part of a banking institute, but it could also be integrated into the administrative structure of an IdP. The PP issues SAML Payment Assertions [3] for validating payment transactions and SAML Payment Tokens that are handled like cash within the federation.

Besides the contractual binding with his IdP, the **Consumer** needs additionally an account at a PP and possibly special hardware or software that has to be used for the token handling and other payment procedures.

The **Payment Token** can be considered to be like a banknote or a coin within the federation. It contains information about the identity of payer, payee and the PP as well as information on currency and the payment's amount. Also, related to security aspects, a lifetime, an identification number, and an issuer's signature are added. The token is issued by the PP on request of a consumer and send by the consumer to the SP for paying requested service access. The SP, in turn, can use the token for other business purposes. Due to the crucial nature of the token, a sufficient security level has to be achieved.

A scenario within such a payment-enabled identity federation can be split up into three different steps: the authentication, the authorization, and the payment. Since authentication and authorization are already established within usual federations, those processes are reused. When the authorization was successful, the SP sends a payment offer back to the consumer, who, in turn, contacts his PP requesting a payment token. After being authorized at the PP, the consumer receives his token, which he may now present to the SP. The SP checks the validity of the token, stores it for further purposes in his database, and allows the user to consume the resource protected.

4 Security Analysis

This chapter considers key security issues for the token-based payment scheme, since a high security level is required for productive uses of the new approach.

The **Identity Provider** cannot start any attack related to the payment, which has not been avoided by standard federation techniques, since the IdP has not been extended with respect to its functionality regarding a non-payment federation.

The **Consumer** shows the weakest piece of the chain in this concept, since he can copy the token and try to double-spend it. Therefore, two approaches can deal with this threat: Detect a misuse or prevent it. If only the detection of misuse is required, it provides for a sufficient security level to ensure that the token is signed correctly to identify the consumer, if he tampered with the token. If the SP wants to exchange the token into money, the PP is able to detect the double-spending. He will hand over the money to the SP, but will charge the consumer for this misbehavior. The prevention of misuse requires hardware-related security such as a Trusted Platform Module or Smart Cards. These systems are able to protect tokens and the application that is used for payment against any attacks from the user. It is an interesting research topic, which of both solutions may fit best.

The **Payment Provider** could try to issue invalid tokens or to refuse exchanging valid tokens. The PP's signature determines the protection against both attacks. If the PP issues an invalid token, this misbehavior will be detected due to its signature. And a valid token must be exchanged by the issuing PP, who can also be detected by its signature on the token.

The **Service Provider** can try to violate the contract. This attack is not specific to the approach of payment in a federation and would invoke penalties. But besides this, the SP can try to attack the infrastructure in the same way as a consumer may do. Thus, further research is needed here as well.

Eavesdropping and the man-in-the-middle attacks are not specific to the payment scenario and may be prevented by using common underlying security technologies, such as X.509 certificates in a trustful Public Key Infrastructure.

A **hardware theft** or **data loss** on consumer's side would be problematic, if the thief is able to pay with the stolen hardware or a data loss would lead to money loss. Basic security ideas like an additional check with a PIN and the revocation of amount reservation if a token is not presented for exchange at the PP within the stated lifetime can avoid that. If the hardware is stolen at SP's side, the thief is not able to reuse the tokens, since they contain information about the payee's identity. But the SP will lose its money because of theft or data loss, if he has no other proof about a transaction, because he cannot claim for exchanging the tokens.

5 Conclusions and Outlook

This paper describes the idea of integrating payment mechanisms into currently established SAML-based federations, which can be done by including the component of a Payment Provider into the federation architecture. Since only few changes in language, protocols, and infrastructure have to be made, this idea is a viable solution to resolve the lack of functionality detected in current identity federations. Apart from the normal payment usage in a federation without having the need to trust an add-on software solution, another important use-case for this approach is the possibility of using micro-payment within the academic

Shibboleth-Federations (e.g., [10], [9]). This provides an incentive for many small commercial service providers to join such a federation.

Since the federation architecture and its infrastructure is already sketched above and designed, the three main topics of further work include the analysis of the exact information that has to be transmitted inside of the Payment Token, a security validation on a high level, and due to the business impact of the idea a cost and acceptance estimation. The analysis of exact information deals with the problem, which information is needed in the token to allow a secure payment process without violating privacy aspects. Security validation is very important within this approach, since a successful attack may lead directly to a loss of money. Regarding the business view, a cost and acceptance estimation should predict, whether the idea could be implemented in practice. Apart from those analytic steps, the approach will also be implemented within a prototype to prove its practicability as well as to take measurements in a validation scenario.

6 Acknowledgement

The approach published in this paper was partly developed in the project SWIFT [7], funded by the EC under the FP7-ICT programme. The authors thank all partners involved in that project.

References

1. D. Chaum, A. Fiat, M. Naor: Untraceable electronic cash. In: Advances in Cryptology - CRYPTO '88. Springer, Berlin Heidelberg New York, pp. 319-327.
2. J. Hughes, E. Maler: Security Assertion Markup Language (SAML) V2.0 Technical Overview. October 2006: http://www.oasis-open.org/committees/download.php/14361/sstc-saml-tech-overview-2.0-draft-08.pdf, 2008.
3. C. Jennings, J. Fischl, H. Tschofening, G. Jun: Payment for Services in Session Initiation Protocol (SIP). 2007: Document ID draft-jennings-sipping-pay-05: http://www.ietf.org/ID.html, 2008.
4. Liberty Alliance Project: Liberty Alliance Project Whitepaper: Personal Identity. 2006: http://www.projectliberty.org/liberty/content/download/395/2744/file/Personal_Identity.pdf, 2008.
5. H. Lockhart et al.: Web Services Federation Language (WS-Federation). Version 1.1, IBM Corporation, December 2006: http://www.ibm.com/developerworks/library/specification/ws-fed/, 2008.
6. OASIS eXtensible Access Control Markup Language (XACML) TC: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml, 2008.
7. Secure Widespread Identities for Federated Telecommunications (SWIFT). Funded by the EC under the FP7-IST programme: http://ist-swift.org/, 2008.
8. Shibboleth Website: http://shibboleth.internet2.edu/, 2008.
9. Switch, The Swiss Education & Research Network: AAI Introductory Tutorial: http://www.switch.ch/proxy/aai/support/presentations/infoday-2006/AAI-ID06-20-Intro.pdf, 2008.
10. Verein zur Foerderung eines Deutschen Forschungsnetzes e. V.: DFN-AAI - Authentifikation Autorisierungs Infrastruktur: https://www.aai.dfn.de/, 2008.