Identity-Based Cryptosystems for Enhanced Deployment of OSGi Bundles

Pierre Parrend, Samuel Galice, Stéphane Frénot, Stéphane Ubéda

Identity-Based Cryptosystems for Enhanced Deployment of OSGi Bundles

Pierre Parrend, Samuel Galice, Stephane Frenot, Stephane Ubeda
INRIA ARES/CITI, INSA-Lyon
F-69621 Villeurbanne, France
E-mail: {pierre.parrend},{samuel.galice},{stephane.frenot},{stephane.ubeda}@insa-lyon.fr

Abstract

The OSGi platform is designed to make Java software extensible at runtime. This undeniably presents a great interest in several domains like embedded platforms or enterprise application servers. However, securing the deployment of the OSGi components, or bundles, proves to be a major challenge. The current approach consists in digitally signing the bundles and certifying the signature through a Public Key Infrastructure.

We propose to replace this technology with Identity-based cryptographic mechanisms, which provide both better performances and simplified key management. We present an infrastructure for initialization and use of Identity-based key management, and define the digital signature of bundles using such a cryptographic scheme. Based on our implementation, we provide a comparison between PKI management and Identity-based Key Management. The proposed approach proves to support radical improvement in the key management process, especially in strongly asymmetric system such as OSGi-based Home Gateway, where a few providers publish services for millions of potential users.

Introduction

Nowadays, the ever-growing connection to Internet of homes and enterprises - often through a connection over ADSL Wide-band Access - brings new capabilities for home entertainments or professional services. The Home Gateway which classically provides the connection to Internet becomes a central device that supports execution of high-level services. These services need to be dynamically loaded on the gateway at runtime, which is supported by the OSGi Platform. The OSGi environment is a lightweight overlay to a Java Virtual Machine. This runtime extension enables new code to be executed on the Home Gateway, and must therefore be strongly protected. This protection is currently performed through the digital signature of the bundles with DSA algorithms, which imply a complex key management. We propose to replace DSA signature with digital signatures that use Identity-based Cryptography. This recent cryptographic scheme enables in particular to dramatically simplify the management of public key, by replacing Public Key Certificates with a string identifier of the signer. A parameter which is specific to the Certification Authority enables every client to deduce to public key from the identifier, and thus to check whether the Certification Authority, called Private Key Generator (PKG) has used a valid private key for the bundle signer.

We present in this paper other works related to secure OSGi and dynamic systems in Section 1, and the principle of Identity-Based Cryptography, in Section 2. The infrastructure for secure deployment of OSGi bundles is presented in the section 3. We then provide a validation of the proposed approach in Section 4, and conclude the paper.

1 Related Works

The security of the component deployment process is enforced is most cases through context-dependent solutions. We provide here an overview of the principal existing solutions.

The default Bundle Signature mechanisms of deployment of OSGi bundles is based on the Java Archive signature [16]. It is strengthened by the OSGi Core Specification Release 4 [11] to provide a higher level of security in the deployment process. In particular, OSGi bundles can not be extended with new resources,

[0] This work is partially funded by MUSE II IST FP6 Project n026442.

when Java Archives can [13]. You can find further technical information related to digital signature of OSGi bundles in [12].

Several alternatives to the OSGi platform have been proposed to support this secure deployment. The Cingal Model [3] manages the deployment of components through insertion of metadata in the components. The bundles are wired together. Each bundle carries authentication metadata, which comprises the digital signature and the identity of the signer. The implementation is not compatible with the OSGi framework, but the principles are very similar. Another alternative is Preatoria [5] which is a framework dedicated to the deployment of Web Services. The security mechanisms are based on the Web-Service standards, which enables to support both deployment and execution time security. Praetoria is developed on the .Net platform. Since it uses Web Service technology, it is less flexible than the OSGi platform. In the context of enterprise systems, the SmartFrog (Smart Framework for Object Groups) [9] has been developed. The security is performed through the encryption of all communications and data transfer. This approach is straightforward in environments where all entities are known, but can not be easily mapped toward large-scale or evolutive systems.

Some solutions are specifically target at the OSGi framework. For instance, Kim *et al.* propose to rely on Message Authentication Code (MAC) based authentication. Consequently, the asymmetric cryptography-based signature with SHA-1 and DSA algorithms is replaced by symmetric cryptography. The creation of a shared secret at bootstrap time is required [7]. This process is more lightweight that the one specified by the OSGi Alliance. However, the use of symmetric cryptography makes the key management more complex and less robust: since the secret key is shared, the non-repudiation of actions can not be guaranteed, keys can be divulgated to third parties, and key revocation is extremely difficult to support. Moreover, the actual benefit is not quantified, which would be of a great interest when choosing to give up the current standard. This work is extended by Lim *et al.* to take advantage of XML technology signature, that supports MAC based authentication [8]. Since XML is usually not considered as a lightweight technology, this extension seems paradoxical with the use of limited resource devices. Again, the lack of quantification of the relative performances of the various solutions does not provide sufficient data to choose between the various solutions.

Identity-based Cryptography has not yet been applied to the deployment of OSGi bundles - or other kind of components. However, several propositions have been made to exploit their possibilities in the context of distributed and pervasive systems. In the context of Health-Care systems - which are a potential applications for Home Gateways - Mont propose to use IB Cryptography to support a secure messaging service [10]. The authors take advantage of the increased flexibility brought by IB Cryptography to enforce role-based security mechanisms. The technology has also been used in the context of the Grid to provide secure communication channels [15].

2 Identity-Based Cryptosystems

Until recently, encryption techniques have relied on long, randomly generated keys that must be mapped to identities using digitally-signed documents, called certificates. The management of these certificates, and the need to fetch a certificate before encrypting to a person or machine, has made encryption very difficult.

Identity-Based Encryption (IBE) takes a completely new approach to the problem of encryption: IBE is a key authentication system in which the public key of a user is some unique information about the identity of the user . That allows any party to generate a public key from a known identity value such as an ASCII string (e.g. a user's email address) enabling data to be protected without the need for certificates. A trusted third party, called the Private Key Generator (PKG), generates the corresponding private keys. Each new user associated to the trusted domain must requests his private key from this PKG. The master key is kept secret by the PKG and there is no authority in charge of the generation of this master key. The PKG controls the mapping of identities to decryption keys in order to ensure the protection of the system.

Historically, the design of a functional Identity-Based Cryptosystem (IBC) was a long-standing open problem in cryptography. The notion of IBC was first introduced by A. Shamir [14] in 1984. In 2001, D. Boneh and M. Franklin [1] were the first to propose a fully adapted model with the help of elliptic curves and the Weil and Tate bilinear pairings serving as building blocks for these Public Key Cryptosystems (PKC).

As a result, parties may encrypt messages (or verify signatures) with no prior distribution of keys between individual participants. This is extremely useful in cases where pre-distribution of authenticated keys is inconvenient or infeasible due to technical restraints. However, to decrypt or sign messages, the authorized user must obtain the appropriate private key from the PKG. A caveat of this approach is that the PKG must be highly trusted, as it is capable of generating any user's private key and may therefore decrypt (or sign) messages without authorization. Because any user's private key can be generated through the use of the third party's secret, this system has inherent key escrow.

The power of IBE is in its simplicity. By using well-known identifiers, such as email addresses, as public keys, IBE enables security policies to be encoded directly into encryption and authentication methods, eliminating the need for cumbersome certificates and Certification Authorities. By eliminating the need for certificates, IBE removes the hurdles of PKI: certificate lookup, life-cycle management, Certificate Revocation Lists, and cross-certification issues. IBE's simplicity also enables it to be used in ways PKI could not: IBE can be used to build security systems that are more dynamic, lightweight and scalable. The IBC based on elliptic curves have numerous advantages as the gain in size of the keys and the reduced computational time. Moreover, they provide as well signature/verification processes as encryption/decryption operations within correct times and for a lower cost of CPU or memory usage than in the case of classical cryptography (as DSA).

We propose thus to utilize IBC to deploy bundle in the OSGi context with a high level of security in parallel. We claim that the resulting protocol is more lightweight in both cost of management and network communications than usual PKC based on traditional cryptographic tools (RSA, DSA). To prevent the natural key escrow problem presents in the native IBE system since the PKG knows each private key, we decide to use the Chang-Zeng-Kim signature scheme which provides a solution to this issue. To support our proposition, we intend to implement a fully functional version of our protocol. The performance of our protocol is comparable to the performance of ElGamal signature scheme. The security of the system is based on a natural analog Extract, Sign and Verify. Considering Alice a signer with her identity d, she signs a message in the Sign phase by using the private key given by the PKG. In the Verify phase, Bob verifies the validity of her signature in an IBS scheme just by using her identity $\mathrm{ID_A}$ and the params made publicly available by the PKG.

The Chen-Zhang-Kim's Identity-based Signature (CZK-IBS) scheme (see [2] for more details about this scheme) is used in the signing and verification phases in order to eliminate the inherent Key Escrow problem as cited in Introduction. This choice is highly motivated by some non-repudiation considerations especially in the context an multi-provider and open environment as the OSGi platform. Another motivation for this scheme is to help the public bundle deployment. Rather than storing a big database of public keys the system can either derive these public keys from a local file or from authorized providers.

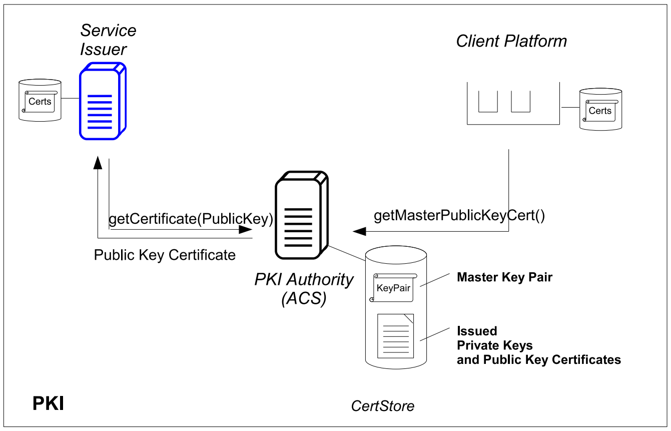

Figure 1. Global view of the initialization of the cryptographic Objects

3 The OSGi Security Architecture with CZK-IBS

The substitution of the classical Public Key Infrastructure (PKI) with an Identity-based key management infrastructure for securing the deployment of OSGi bundles has two main advantages. First, the process of key management is greatly simplified, which makes the actual use of secure deployment more realistic than with a PKI [4]. Secondly, the specifications of this new deployment scheme provides a support to extend the original functionalities with the confidentiality of the bundles. Three phases need to be specified for the deployment of CZK-IBS signed bundles: the initialization of the cryptographic objects, the process of bundle deployment, and the mechanisms of bundle signature.

3.1 Initialization

Initialization of the cryptographic objects in our infrastructure is shown in the figure 1. The process is the following.

First, all entities that need to be identified must be initialized. The parameters of the trusted PKG which performs the management of cryptographic objects in our infrastructure must be distributed through a secure channel to all participants, along with their own unique identifier. This is typically done offline. In the context of telecommunication services such as those developed in the Muse Project, the PKG is located on the Access Control Server. The identifier delivered to the participants of the system contains the following information: a unique string identifier. The PKG stores a copy of the public identities to be able to identify valid participants. This offline initialization of cryptographic objects is typically done through a USB key or a smart card where the specified informations are stored. This pre-identification step is mandatory in closed systems, such as Home Services, monitoring systems, or enterprise informations systems. It can be by-passed in open systems such as the deployment of open source software or in ambient systems, where all actors that want to take advantage of the infrastructure should be allowed to. While allowing unknown entities to be identified, such an approach guarantees the uniqueness of the bundle providers, and thus prevents both the tampering of the bundles and the impersonation of the providers.

Secondly, the bundles Issuers retrieve their private key from the PKG. Therefore, the PKG is implicitly granted a strong trust, since it could forge any private key of all entities that rely on it. Nevertheless, the CZK-IBS provides a tracing scheme to detect the PKG's impersonation. The retrieval of the private key must be performed again when the issued private key is expired. Typically the span-life of a private key would be a short period of time, such as a day or a week. This short validity of time of the private key makes the revocation of the issuers a lightweight process, since it is sufficient not to issue a new private key for them.

Thirdly, the client platforms are initialized. A client needs two types of data so as to subsequently check the validity of the bundles it loads. The first type, the so-called 'params' of the PKG must be known. They allow to compute the public key of each bundle issuer from their identity and above all, to verify the signature of the signed bundles. The second type of data is a list of trusted bundle issuers that are considered as valid must also be available. Otherwise, it would be possible for any malicious issuers to sign and publish bundles that would be considered as valid.

3.2 Bundle Deployment with CZK-IBS

The process of deployment with CZK-IBS scheme is shown in the Figure 2. It is very similar to the one in the context of a classical PKI, with a notable gain in term of management complexity.

The signature phase is similar to the signature mechanism in the PKI based model. The differences lay in the cryptographic algorithms that are used (see section 3.3) and the frequency of the update of the private key of the signers. The validation phase is done in the same way as in the case of the PKI. The validation process must be adapted to the algorithms. The validation of the public key certificate is replaced by the control of the validity of the identity of the signer: its identity is compared against the list of valid signers that has been obtained during the initialization phase.

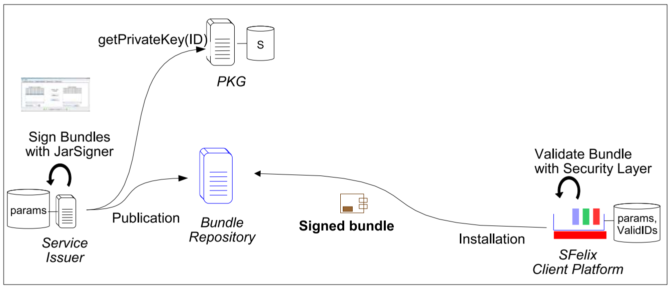

Figure 2. Secure Deployment of OSGi Bundles with CZK-IBS scheme

The confidentiality is achieved by encrypting the bundles before their publication. Because it is not possible to publish a signed bundle for all clients, groups must be defined that gather the client platforms with similar functional and trust profiles. The clients retrieve the private key of their group through a request to the PKG. Consequently, this latter must maintain a list of the users' identities for each group. The withdrawal of clients from the group is dealt with by a regular key update. Former group members can not have access to the new keys. The total number of groups should be reduced, so as to limit the number of copies of a single bundle that are encrypted with different public keys. Moreover, the user authentication mechanism is also based on its identity.

3.3 Bundle Signature with CZK-IBS

The process of signing bundles is pretty similar to the classical one [12]. The algorithms used for obtaining the hash values are the same but those generating the digital signature are different. Into the bargain, the absence of a public key certificate makes the CMS format [6] obsolete. The structure of a signed bundle using CZK-IBS scheme is depicted in the figure 3. Each resource of the archive is identified in the **META-INF/MANIFEST.MF** file, along with its hash value. So as to allow several signers to sign the bundle, the hash value of this Manifest file is stored in a so-called **Signature File**, as well as the hash value of the various entries of the Manifest. The digital signature itself is realized on the Signature File, and stored

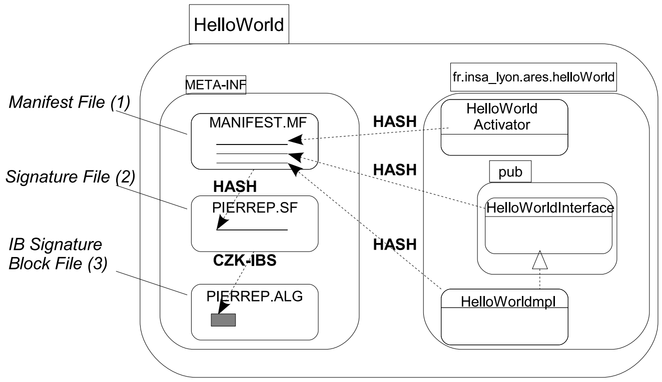

Figure 3. Structure of a signed bundle, using Identity-based Cryptography

in the **Signature Block**.

We propose to replace the CMS compliant Signature Block by an **IB-CMS** compliant block, that is to say a modified CMS file that contains the information related to the signer, such as its identifier, and the properties of its key, such as the period of validity. The signer informations are the following: the signer identifier ('signerID'), the identifier of the PKG that issues the private key ('keyissuerID'), the date of the emission of the key (with the year, the month, the day), the validity period of the key (an integer value, and a time unit, which can be day, week, month or year), and the name of the algorithms that are bound to this key. The encryption algorithm is mandatory. In most case, the hash algorithm is bound to the encryption algorithm, and must be specified. The CZK-IBS scheme is also integrated in the IB-CMS file. Since it is based on Elliptic curve cryptography, it is more performant and more compact that the classical DSA one. Two fields are removed from the original specified format, because they make no sense in the context of IBC: the X.509 public key certificate (or list of certificate, if delegation of signature was provided), and the Certificate Revocation List (CRL). Consequently, the IB-CMS file is more lightweight than the CMS one was, which can be a useful property in environments with limited resources.

The substitution of classical PKI-based asymmetric cryptography by the Identity-based scheme makes it possible to build an infrastructure for secure deployment of bundles that is both easier to manage, and less greedy in term of resource consumption. We claim that these two properties not only bring an improvement to the current specified solution, but also that it merely makes it a realistic choice for systems that are both complex and limited in their resources.

3.4 Security Analysis

We present in this section a short security analysis of our infrastructure against some classical attacks. The basic security properties a cryptosystem should provide are Confidentiality, Integrity, Authentication, and Non-repudiation. Confidentiality is keeping information secret from all other than those who are authorized to see it. Integrity is ensuring that the information has not been altered by unauthorized or unknown entities. Authentication is the assurance that the communicating party is the one that it claims to be. Non-repudiation is preventing the denial of previous commitments or actions. The security of each cryptographic primitive used in our proposition was discussed in the referenced paper [2] and was clearly established. Although the first IBC security notions were proposed in [1], there is no work yet aiming at establishing the strength of this notion in a full security analysis. So far, only the indistinguishability based security notions, as well as their variations have been considerated in the literature.

Digital Signature is a fundamental cryptographic primitive which provides authentication, integrity and non-repudiation. The unforgeability of the hashed message guarantees the integrity of the CZK-IBS Signature. This property is provided by the collision resistant property of the hash function used. Due to recent results published in [17], at least SHA-1 must be used to be sure that the hash function does not permit to compromise the bundle signature integrity.

In our proposition, the PKG plays an important role by defining entirely the security domain and thus may potentially forge signature for any message. Nevertheless, the CZK-IBS scheme provides a way to circumscribe this problem. The dishonesty of the PKG can be proved by the Service Issuer by providing a proof of his secret key $(\mathrm{S}_{\mathrm{ID}_A}, r)$ through a knowledge challenge. So there is Authentication in the system.

The PKG also plays an important role by ensuring that all the valid Service Issuers are trustworthy. Actually, the Service Provider in an OSGi based Service Environment exists outside the home network as does the Home Gateway manager for managing the home gateway and authenticating the users. Our protocol is designed under the assumption that Identity-based Infrastructure is used according to Home Gateways storage and computation capabilities, the params are shared between all entities. Another assumption is that the service users trust the Service Manager. Finally, Home Gateway knows that the PKG is legitimate by using its public key initialized in a preinstallation phase.

4 Validation

The validation of our approach is performed in two steps. First, we present the technology that we use to develop our prototype. Then we perform an qualitative and quantitative evaluation of the benefits of Identity-based cryptography in the process of secure deployment for OSGi Bundles.

4.1 Implementation

A prototype for IB Cryptography systems is currently being built at the CITI Laboratory. It will be integrated with the SFelix suite we previously developed[1], which is an implementation of current OSGi Release 4 specifications of Bundle Signature.

The SFelix suite is written in Java, to be fully compliant with the OSGi environment. However, current implementations of identity-based cryptography libraries, Miracl and Voltage, are only available in C. This does not prevent experimentation, since call to native libraries are well supported in Java, but limits the portability of the solution.

We now discuss the existing IB cryptographic libraries. The first implementation is based on Miracl which is a portable C/C++ library providing a full implementation of Multiprecision Arithmetic. In particular it includes all the primitives necessary to implement Number Theoretic based methods for Public Key Cryptography, such as Diffie-Hellman, RSA and DSS. Complete support is also provided for implementation of Elliptic Curve Cryptosystems over the fields GF(2m) and GF(p). The MIRACL big number library also contains an experimental implementation of IBE[2]. The second implementation is based on Voltage IBE Toolkit which is a set of tools that enable developers to quickly and easily incorporate Identity-Based Encryption into their applications. Using the Voltage IBE Toolkit, applications can seamlessly integrate with the Voltage Security platform and take advantage of its centralized administration, advanced policy management, and key distribution architecture[3].

Our IB-based digital signature tools are in their early development stage. However, this does not prevent us to perform a precise evaluation of the proposed framework.

4.2 Benefits for Security Management

The prototype we develop allows us to evaluate the actual benefits of Identity-Based Cryptography in the process of deploying OSGi Bundles. This evaluation makes it possible both to confirm that Identity-Based Cryptography hold its promises, and to draw actual pros and cons of classical PKI-based systems and IB-Crypto based systems.

A systematic comparison between Classical PKI and Identity-Based Cryptography PKI is given in Table 1. The first main difference, which is the ground if the simplicity of management of IB-PKI systems, is that the public key must be disseminated as is in the context of classical PKI, and that it is directly deduced from a string identifier and from a Private Key Generator specific parameter with IB-Cryptography. Consequently, keys are updated using huge periods in classical PKI, whereas they can be updated daily with IB-Crypto: if a time stamp is appended to the signer's identifier to generate the public key, this latter can be updated daily. The client only needs to re-generate locally the new public key. The benefit of regular key update is that public key revocation is performed transparently. When a signer is no longer part of the system, she can not retrieve a new daily key pair from the PKG. So she can no longer sign bundles. On the contrary, classical PKI infrastructures imply that the client must be notified when a signer is revoked, and thus complex Public Key Revocation mechanisms must be available. Moreover, Key size and time for signature verification are decreased with IB-Cryptography.

PKI based on RSA or DSA algorithms still have advantages over Identity-based Cryptography. In particular, the speed of signature generation is greater using DSA or RSA algorithms. But the main drawback of Identity-Based Cryptography is that the Private Key Generator must be fully trusted, since he knows the private key of all entities of the systems. Whereas classical PKIs are based on the certification of public keys: they validate this latter without having access to the private key. Thus, the Certification Authority requires a lower trust level than PKGs. We solve this problem by using the IB-CKS cryptographic scheme, which makes key escrow traceable, and therefore forces the PKG to be honest.

A quantitative analysis shows that Digital Signature of Bundles using IB Cryptography provides a great enhancement in key management overhead when compared to PKI infrastructure. When a new key is used by a signer, this latter makes a communication with the PKG to retrieve the new private and public keys. Assume that N signers are authorized to publish bun-

[1] http://sfelix.gforge.inria.fr/

[2] http://www.shamus.ie/

[3] http://developer.voltage.com

dles in the systems, this is tantamount to N communications - a reasonable assessment is than N is of the order of magnitude of 10, or even less. When a client loads a bundle, it can check locally that the key is valid and has been issued by the trusted PKG. So no communication with the PKG is required. The total number of communication with the Certificate Authority is thus N. In the context of PKIs, the signers need to certify their Public Key Certificates, which amounts to N communications. When they load a new bundle, the clients must check that this Public Key has not been revoked. This is done through a request to the Certification Authority, which provides a Certificate Revocation List (CRL). The number of client is noted M, with M of the order of magnitude of a couple of million, if we assume as in the Muse European Project that the Home Gateway is provided with the ADSL modem (in France, the number of client varies between 1 and 5 millions clients for each ADSL providers). On the first hand, the PKG must stand a traffic of some tens of connections daily. On the other hand, the PKI must be available for several millions of users. If the PKI is replicated on the DSLAMs, each replica serves no more than 400 clients, but all DSLAMs must support CRL functionalities, which obviously causes an important system update overhead. Identity-based Key Management systems therefore has a radical technical advantage over PKIs, which could soon be translated in radical financial gains for telecommunications firms.

Since we have developed prototypes for both DSA-based digital signature and Identity-based systems, it would be of interest to compare the relative computation speed of both techniques. However, the Bundle Digital signature we use is written using the Bouncycastle Java library for DSA-signature, and the Identity-based Cryptographic C libraries are accessed from Java code through native calls. Quantitative comparison would be a comparison of C and Java more than an evaluation of both techniques. We intend to perform these evaluation as soon as a Java implementations of Identity-based Cryptographic tools are available.

PKI and IB Cryptography have both pros and cons what concerns cryptographic and system security properties. But the simplification in the key management process with Identity-based systems, which allows client to check digital signatures without any need to contact a certification authority proves to allows dramatic key management gains, in particular in strongly asymmetric systems such as telecommunication Home Gateways.

	PKI		IB-PKI		**Ratio**
	+	-	+	-	
Key Management		Public Key Dissemination	Public Key is Identifier		
Key Revocation		Heavyweight	Transparent, through regular key update		
Cryptographic Operations	Signature Speed		Key Size, Signature Verification Speed		
CA Trust Level	High			Key Escrow Risk if untrusted	
Number of Coms with the CA		N+M	N		→ $1/M$

Table 1. Pros and Cons of classical PKI and IB-PKI Approaches

5 Conclusion and Perspectives

We have proposed in this paper a protocol to secure the deployment of OSGi bundles by using recent cryptographic algorithms based on elliptic curves and bilinear pairings. Our proposition relied on the CZK-IBS scheme to support the Public Key Infrastructure (PKI) instead of the classical solutions as those specified by the OSGi Alliance. The use of Identity-based cryptography has several advantages: first, the key management overhead is greatly reduced, which can provide a radical advantage in the case of strongly asymmetric systems such as Home Gateway infrastructures, where a couple of providers publish services for an important number of clients. The public keys do not need to be published, since they can be deduced from the identifier of their owner. Moreover, the complex revocation scheme vanishes and is replaced by the frequent update of the keys, typically every day or week. Another advantage of our proposition which has probably a less radical impact is the fact that the keys and signatures used are based on Elliptic-curve cryptography. They are therefore more compact than those bounded with the DSA algorithm which is currently used for signing archives. We have also defined in this paper the process for securing the deployment of OSGi bundles using Identity-based cryptography, as well as the structure of a signed OSGi bundle by the CZK-IBS scheme. Both qualitative and quantitative benefits of the approach were discussed. Yet, our approach has some limitations, in particular the centralization of the security scheme around the PKG, which becomes a single point of failure. Its compromission means a high impact on the overall security of the system.

However, we believe that Identity-based Cryptography enables to greatly reduce the key management overhead, and thus may succeed in large scale systems where PKI have so far proven to be very difficult to manage.

References

[1] D. Boneh and M. K. Franklin. Identity-based encryption from the weil pairing. In *Advances in Cryptology - Crypto'2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 213–229. Springer, 2001.

[2] X. Chen, F. Zhang, and K. Kim. A new ID-based group signature scheme from bilinear pairings. In *Information Security Applications, 4th International Workshop - WISA'03*, volume 2908 of *Lecture Notes in Computer Science*, pages 585–592. Springer-Verlag, 2003.

[3] A. Dearle, G. Kirby, A. McCarthy, and J. D. y Carballo. A flexible and secure deployment framework for distributed applications. In *Lecture Notes in Computer Science 3083*, pages 219–233. Springer, 2004.

[4] C. Ellison and B. Schneier. Ten risks of pki: What you're not being told about public key infrastructure. *Computer Security Journal*, 16(1), 2000.

[5] M. Gaedke, J. Meinecke, and M. Nussbaumer. Supporting secure deployment of portal components. In *ICWE 2004*, number 3140 in LNCS, pages 516–520, 2004.

[6] R. Housley. Cryptographic message syntax (cms). IETF RFC 3852, July 2004.

[7] Y.-G. Kim, C.-J. Moon, D.-H. Park, and D.-K. Baik. A mac-based service bundle authentication mechanism in the osgi service platform. In *DASFAA*, volume 2973/2004 of *LNCS*, 2004.

[8] H.-Y. Lim, Y.-G. Kim, C.-J. Moon, and D.-K. Baik. Bundle authentication and authorization using xml security in the osgi service platform. In *ICIS '05: Proceedings of the Fourth Annual ACIS International Conference on Computer and Information Science (ICIS'05)*, pages 502–507, Washington, DC, USA, 2005. IEEE Computer Society.

[9] C. Low and J. Guijarro. A smartfrog tutorial. Hewlett-Packard Development Company Whitepaper, July 2006.

[10] M. Mont, P. Bramhall, and K. Harrison. A flexible role-based secure messaging service: Exploiting ibe technology in a health care trial. In *14th International Workshop on Database and Expert Systems Applications, DEXA 2003*, pages 432–437, 2003.

[11] OSGI Alliance. Osgi service platform, core specification release 4. Draft, 07 2005.

[12] P. Parrend and S. Frenot. Secure component deployment in the osgi(tm) release 4 platform. Technical Report RT-0323, INRIA, June 2006.

[13] P. Parrend and S. Frenot. Supporting the secure deployment of osgi bundles. In *First IEEE WoWMoM Workshop on Adaptive and DependAble Mission- and bUsiness-critical mobile Systems, Helsinki, Finland*, June 2007.

[14] A. Shamir. Identity-based cryptosystems and signature schemes. In *Proceedings of CRYPTO 84 on Advances in cryptology*, pages 47–53, New York, NY, USA, 1985. Springer-Verlag New York, Inc.

[15] T. Stading. Secure communication in a distributed system using identity based encryption. In *3rd IEEE/ACM International Symposium on Cluster Computing and the Grid, CCGrid 2003*, pages 414–420, 2003.

[16] Sun Microsystems, Inc. Jar file specification. Sun Java Specifications, 2003.

[17] X. Wang and H. Yu. How to break md5 and other hash functions. In *Advances in Cryptology - Eurocrypt'2001*, volume 3494 of *Lecture Notes in Computer Science*, pages 19–35. Springer, 2005.