Security and trust issues in ubiquitous environments - the business-to-employee dimension[1]

Thomas Walter[(*)], Laurent Bussard[(**)], Philip Robinson[(***)], Yves Roudier [(**)]

[(*)] DoCoMo Euro-Labs
Landsberger Strasse 312,
D-80687 München, Germany
walter@docomolab-euro.com

[(**)] Institut Eurécom
2229 Route des Crêtes
06904 Sophia Antipolis, France
bussard@eurecom.fr
roudier@eurecom.fr

[(***)] SAP AG, CEC Karlsruhe
Vincenz-Prießnitz-Str. 1,
D-76131 Karlsruhe
philip.robinson@sap.com

Abstract

Ubiquitous applications and services combined with mobile business applications define a challenging context for security and trust. Besides the basic security requirements for controlled access, confidentiality, data integrity and accountability it is essential to know whether devices surrounding a user are trusted and to distribute application tasks between those devices. We propose a development framework that combines security policies, certificates and an enforcement protocol as a solution to provide security and trust in ubiquitous applications and services.

Security policies define the constraints when, how and which mobile devices can be use in a mobile business application. Enforcement of policies makes use of certificates, defined for users and devices, which determine delegable application tasks and trustworthiness of devices. Our proposed framework is flexible – can be dynamically changed, is adaptable – can be dynamically extended, and is scalable – policies and certificates are evaluated on demand and in a distributed fashion.

1 Introduction

The ever-increasing adoption of mobile devices and wireless communications technologies are the driving forces that open new business opportunities and working models as well as infrastructure technologies “ambient intelligent space” [5]. Companies may enable their workforce, business partners and customers with mobile access to corporate resources such as corporate networks, data and applications. Traditional business activities and tasks can be “outsourced” so that these can be performed from anywhere, anytime and irrespectively of context. The potential gains of mobile services and applications may however be outweighed by the additional effort necessary in order to protect company assets. In this paper we present a framework and discuss basic concepts that can be utilised to implement security and trust in mobile business applications and thus enhance the value of conventional communications.

Security here implies protecting corporate resources against threats and attacks. Access control, data confidentiality and integrity, availability of services and accountability of actions (also referred to as non-repudiation) [3] [6] are security goals that help to defeat against threats and attacks. Trust is meant as an indication that an entity fulfills its commitments; e.g. that a device does not reveal confidential data.

With ubiquitous services and networking any security and trust enabling solution has to be adaptable; this basically comes from the fact the numbers of users, devices or administrative domains are a priori

[1] WiTness – Wireless Trust for Mobile Business – is supported by the European Commission under grant FP5 IST-2001-32275 [9].

unpredictable. Consequently, requirements as well as administrative and management issues are diverse.

State-of-the-art solutions such as firewalls [6] and virtual private network [8], however, do not provide flexible and scalable solutions. Firewalls protect a network from unauthorized access and perform traffic filtering but provide nothing or little in order to protect data transfer. Virtual private networks are good in access control and protecting data transfer but do not guarantee seamless access (without implying a serious work load on network administrators). Access control generally relies on access control lists that are difficult to manage when multiple domain are involved. Additionally, virtual private networks support confidentiality and data integrity, but do not implement non-repudiation of communication events or business transactions.

To achieve the required adaptability we propose a security and trust framework that has at its heart a language to define security policies [1] [7] and authorization and trust certificates [2]. Policies constrain the behavior of servers in the corporate domain as well as the behavior of mobile devices (such as phone, laptops, personal digital assistants, etc.) or combination of mobile devices. The trustworthiness of mobile devices and how they can be used by employee is controlled by trust and authorization certificates, respectively. In this paper we describe the mutual dependency of policies and certificates and their combined use.

The paper is structured as follows: Section 2 defines ubiquitous business scenarios and the resulting security requirements. In Section 3 we discuss our framework and we give details on how to set up a secure distributed application platform. Security policies and certificates, the two basic elements of our approach, are discussed in Section 4. Before concluding, Section 5 provides concrete example.

2 Security and trust in ubiquitous business-to-* scenarios

From our perspective, ubiquity in business-to-* (B2*), e.g. business-to-consumer or business-to-employee, can be viewed as both a movement towards ubiquitous access to corporate resources and ubiquitous access to devices. Ubiquity gives mobile users and workers the freedom to access essential business services and data irrespective of location and technical infrastructure at hand. Basically, any mobile device, any device offered by the environment (e.g. printer in an airport, display in a plane), or combination of devices can be used in order to perform assigned business tasks. The selection of devices to be used may take into account user's or the company's preferences with respect to usability, performance, networking capabilities etc. The concrete decision rests with an evaluation of the configuration that best fits the user's requirements.

2.1 Pervasive sales manager example

By way of example, we picture a travelling salesperson using a personal digital assistant (PDA) to administer customer contact information and meeting schedule. In order to update contacts and personal schedule (agenda) he or she connects to the corporate network via a GPRS (general packet radio service) enabled mobile phone. Alternatively, the salesperson receives a spreadsheet with latest sales figures on the mobile phone and transfers this data to a notebook or a public terminal in order to have a suitable device to display and to browse the spreadsheet.

2.2 Security and trust in business-to-employee

In business-to-employee (B2E) scenarios, mobile business applications demand trusted connectivity of clients and services regardless of the available devices, infrastructure and networks. These may be

dynamically and even implicitly assembled by the mobile worker, whose goal is to complete the corporate tasks assigned. Trusted implies an availability of user and service credentials, policies that assess the attributes of these credentials, and the resultant strict designation of permissions [7]. The generalized application security requirements are therefore:

- Mutual authentication of clients and server,
- authorization of users and applications to use corporate resources, as well as
- data confidentiality and integrity, and non-repudiation of communication events (i.e. logging) and transactions (e.g. order approval).

Although we have paid special attention to B2E scenarios, the following results show potential for generalization and applicability in arbitrary mobile business scenarios.

3 Security framework – basic elements

The framework presented in this paper stipulates a set of base constraints for the bootstrapping of secure communications and resource sharing between applications hosted on mobile devices and the application services within the corporate network.

3.1 Federations

Our definition of a *federation* builds upon the circumstance of devices forming collaborative networks, where the roles of nodes are selected (priori or ad hoc) on the basis of capability and trust. Subsequently, this capability is often represented by the software elements installed on the devices, such that a federation is also a network of selective application functionality. Thirdly, the term federation implies the presence of governance, which rests with the commitment of the federative peers to a set of security policies (see below for a discussion of the term *security policy*).

The term federation is therefore a matter of relationships between communicating nodes, whether the inter-nodal connectivity is represented by a client/ server environment, a system of personal device peers, or an ad hoc, discovery-based combination of mobile, shared and public devices, with possibly different owners. In either context the security requirements homogeneously remain as those of the overall application, and are to be met as defined by the respective security policies. A federation thus extends the concept of a trusted platform beyond a single entity to a distributed topology. However, we maintain that there must be at least one core component that provides support for offline or online security services.

Every mobile device stores its own private and public key pair, corresponding public-key certificates and trust certificates. Trust certificates describe the trustworthiness of the device (more details will come below). The security framework (security module, certificates and policies management tools, etc.) is preinstalled.

3.2 Assumptions

For a federation of mobile devices the following assumptions apply:

- A security module (a trusted hard- and software component dedicated to security operations) must be available. The security module holds the employee's private and public key pair(s), public-key certificate(s), root certificates as well as authorization certificates. The latter determine the rights of

an employee with respect to delegation of business tasks which may be allowed or disallowed. Root certificates allow the validation of (third-party) certificates. Private and public keys and all certificates are generated by the company and stored on the security module before the security module is handed over to the employee.

- A robust bearer device must be appointed; this is the physical host of the security module. For this role, we suggest specialized devices (as opposed to multi-purposed) that possess a minimalist peripheral and user interface, thereby providing some measure of tamper-resistance.

- Other federated devices must support some form of peer-to-peer communication. Although not required (i.e. a wired communication infrastructure may do as well) we assume that devices support at least one wireless communication technology such as infrared (IrDA), Bluetooth or WLAN.

4 Certificates and security policies

This section describes how security policies are defined and enforced. Security policies related to authorization and trust are implemented as certificates: an extension of the simple public key infrastructure [4] deals with authorization and trust. The allowed combination of mobile devices into a federation and the sharing of resources in a federation and between federation and corporate network is controlled and protected by security policies and certificates.

4.1 Certificates

Certificates are signed data items that are used during different phases of the federation lifecycle. Besides public-key certificates, our framework uses two other types of certificates: authorization and trust certificates. These certificates have basically the same structure but are used and resolved differently; for more details on this topic see [2].

4.1.1 Authorization certificates

Authorization certificates are role-based and bound to employees (Figure 1). They determine the role of an employee and his or her rights. For instance, an employee in the role of a salesperson may have access to the customer address data base and his or her personal schedule. An employee in the role of a sales department manager has the right to access the order database, to perform approval of orders and to revise budget figures. The sales manager may also be entitled to delegate certain task, e.g. the task of approving orders.

4.1.2 Trust certificates

Trust certificates are assigned to devices (Figure 1). They provide evidence on the trustworthiness of devices. We can think of a situation where secret data should only be processed on devices that come from the employee's company. Before delegation of a task to another device takes place the device's trust certificate is evaluated. If the certificate proves that the device is owned by the company and is trustworthy then application task and data are delegated and are transferred to the respective device.

However, co-operating companies may mutually agree to maintain an appropriate security and trust level on their devices. Then some tasks and data may be shared among devices that are owned by

different companies. In this case chains of trust certificates are evaluated to establish trust levels. However, all this is controlled by respective security policies (see below and Section 5 for an example)

Certificates are static data assigned to entities – employees and devices. They are evaluated online during runtime of a distributed application against requirements that are stated in security policies.

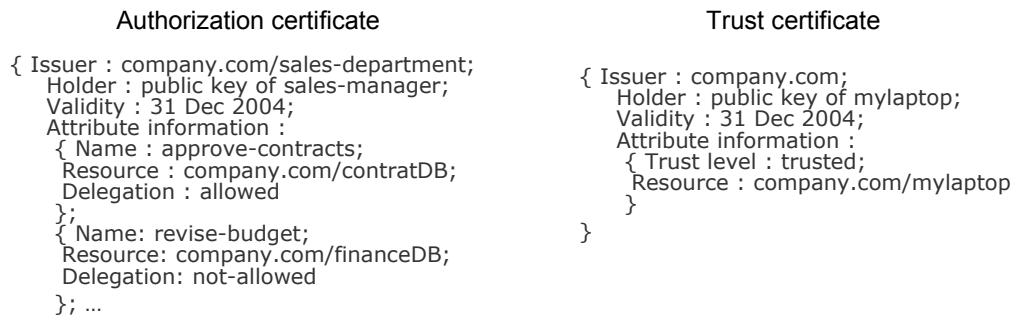

Figure 1: Authorization and trust certificates

4.2 Security policies

The framework also facilitates an encoding of security policies at a higher-level than certificates, which specifies the constituents of the associated application's security context. Security policies are therefore application resources defined during the application development and integration process and are bundled with an application when the application is being (pre-) installed within the corporate network as well as on mobile devices. The security context is created when the application is installed, through a process of querying various resource profiles on the host device for the mechanisms that satisfy the policy specification. The resultant security context is a data structure of security service invocations, mapped on to specific modes in the application's runtime.

We identify four types of security policies defined in our framework, namely authorization, configuration, delegation and federation (Figure 2). The latter three policy types belong to the core of the framework; however, we include the authorization policy for completeness.

Authorization policies typically exist within a corporate network and control the access to resources within the network. The *configuration policies* are representative of the authorization policies of the corporate network. Furthermore, the functionality of an application assigned to one principal "A" (e.g. sales manager) may also be delegated to another principal "B" (another sales-department manager). The framework therefore specifies a *delegation policy* that states the rules, for example, what evidence does "B" have to supply "A" before the task can be delegated. These are known as assertions; authorization certificates as discussed above are used in this context. Additionally, an application "P" may require that an application "Q", either on a local or remote federated device, be assigned the handling of a subtask of the application. The framework specifies the *federation policy* for providing assertions regarding the validity of devices to be included in such assignment. Trust certificates are the container that store information on devices, which is evaluated against federation rules.

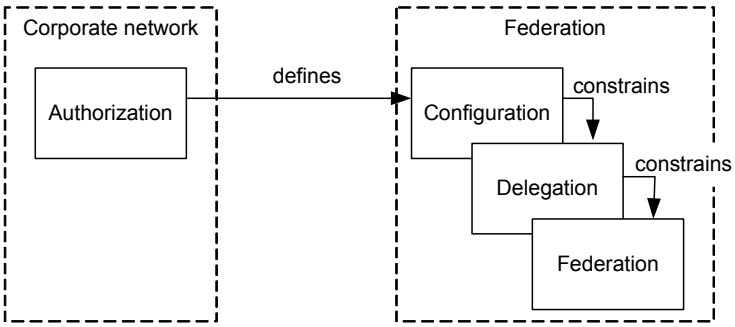

Figure 2: Security policies

5 Example – the pervasive sales manager

For the example introduced in Section 2.1 we discuss a concrete policy specification and enforcement.

5.1 Security policy specification

An authorization policy defines that network access is only given to authenticated clients. The details how authentication is achieved are not further presented here. A distributed interpretation of this authorization policy into a configuration policy defines that mutual authentication using public-key certificates and SSL protocol are used. An extension of this configuration policy would be given by a delegation policy asserting that delegation is only done for a task, e.g. approving an order, which the employee, e.g. a sales manager, has permission to delegate (this is specified in the authorization certificate of the employee) and that the recipient of the delegation has the required role, i.e. must be a sales manager (this information is again defined in the respective authorization certificate); for both see Figure 1.

A federation policy, furthermore, may restrict the scope of delegable devices; e.g. trusted devices in the same federation but not un-trusted public devices like terminals and printers (see also below for further details).

5.2 Security policy enforcement – federation policy

Figure 3 gives an example of a federation policy. The meta-data includes its name (“federate-approve-contracts”), issuer’s signature and validity. However, the core elements specified are:

- the SCOPE of federative devices: “SECRET”, any device in an employee’s personal area network, “CONFIDENTIAL”, any device of even different employees of same company, or “PUBLIC”, unrestricted. For instance, SECRET means "trusted enough to deal with secret corporate data".

- the ASSERTIONS how a specific permission is validated: the “trust” level is evaluated by checking the device’s “trust certificate”; to perform the evaluation of the certificate a specific “trust evaluation” method is to be used.[2]

[2] The respective implementation of mentioned method has to be provided in our framework.

FEDERATION (federate-approve-contracts) {
SCOPE: "SECRET"
ASSERTION: SEC.trust, SEC.trust_evaluation(), SEC.trust_certificate
ISSUER-SIGNATURE: signature.of.company.com
LIFETIME: 31 Dec 2003 - 00:00 GMT }

Figure 3: Federation policy

Assuming a trust certificate as shown in Figure 1, it is checked to whom the device belongs and what the trust level of the device is. Both are done by using the trust certificate attribute values "Trust level" and "Resource". The device belongs to the corporation and the trust level is "trusted". The first property is essential for assessing the correct SCOPE (= SECRET, i.e. only own devices may be federated). Because the devices belong to the employee and it is trustworthy ("Trust level: trusted"), the device may be federated and receive some application tasks to execute.

6 Conclusions

We have presented a development framework that enables secure mobile business applications in ubiquitous environments. Applications may run on federations of mobile devices. Federated mobile devices may either provide ubiquitous applications and services. Our framework provides the required means to control the use of mobile devices to avoid disclosure of company secrets (either data or applications). The framework incorporates two elements: security policies and certificates. Security policies are defined by a company to specify applicable security requirements for diverse business applications. Certificates provide the means to determine authorizations and trust of employees and devices, respectively. Policy enforcement provides a link between both elements. Federations between mobile devices and the distribution of application tasks between federated devices comply with the security requirements set forth in applicable policies.

References

[1] M. Blaze, J. Feigenbaum, J. Ioannidis, and A. D. Keromytis; The KeyNote Trust Management System Version 2; Internet RFC 2704, September 1999.

[2] L. Bussard, Y. Roudier, R. Kilian-Kehr, S. Crosta; Trust and Authorization in Pervasive B2E Scenarios; Proceedings of the 6th Information Security Conference (ISC'03), Bristol, United Kingdom, October 2003.

[3] H. B. DeMaio; B2B and Beyond – New Business Models Built on Trust; John Wiley & Sons, 2001.

[4] C.M. Ellison, B. Frantz, B. Lampson, R. Rivest, B.M. Thomas and T. Ylonen, SPKI Certificate Theory, RFC 2693, 1999, expired.

[5] IST Advisory Group; Trust, dependability, security and privacy for IST in FP6; European Commission, ftp://ftp.cordis.lu/pub/ist/docs/istag_kk4402464encfull.pdf, June 2003

[6] W. Stallings; Cryptography and Network Security – Principles and Practice; Prentice Hall, 1999.

[7] M. S. Sloman; Policy driven management for distributed systems; Journal of Network and Systems Management, 2(4):333--360, 1994.

[8] R. Sutton; Secure Communications – Applications and Management; John Wiley & Sons, 2002.

[9] WiTness; Wireless Trust for Mobile Business; FP5 IST-2001-32275, www.wire-less.trust.org.

