

# **Technical White Paper BlueX**

## **The Concepts of BlueX explained**

This document contains information of a proprietary nature.  
No part of this document may be reproduced or transmitted in any form or by any means electronic, mechanical or otherwise, including photocopying and recording for any purpose without written permission of A.E.T. Europe B.V.  
Individuals or organisations, which are authorised by A.E.T. Europe B.V. in writing to receive this information, may utilise it for the sole purpose of evaluation and guidance.

**A.E.T. Europe B.V.**  
**IJsselburcht 3**  
**NL - 6825 BS Arnhem**  
**The Netherlands**

## Warning Notice

---

All information herein is either public information or is the property of and owned solely by A.E.T. Europe B.V. who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

This information is subject to change as A.E.T. Europe B.V. reserves the right, without notice, to make changes to its products, as progress in engineering or manufacturing methods or circumstances warrant.

Installation and use of A.E.T. Europe B.V. products are subject to your acceptance of the terms and conditions set out in the license Agreement which accompanies each product. Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/ or industrial property rights of or concerning any of A.E.T. Europe B.V. information.

Cryptographic products are subject to export and import restrictions. You are required to obtain the appropriate government licenses prior to shipping this Product.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, A.E.T. Europe B.V. makes no warranty as to the value or accuracy of information contained herein. The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, A.E.T. Europe B.V. reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

A.E.T. EUROPE B.V. HEREBY DISCLAIMS ALL WARRANTIES AND CONDITIONS WITH REGARD TO THE INFORMATION CONTAINED HEREIN, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL A.E.T. EUROPE B.V. BE LIABLE, WHETHER IN CONTRACT, TORT OR OTHERWISE, FOR ANY INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER INCLUDING BUT NOT LIMITED TO DAMAGES RESULTING FROM LOSS OF USE, DATA, PROFITS, REVENUES, OR CUSTOMERS, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF INFORMATION CONTAINED IN THIS DOCUMENT.

© Copyright A.E.T. Europe B.V., 2004 - 2005.

All rights reserved.

BlueX is a trademark of A.E.T. Europe B.V. All A.E.T. Europe B.V. product names are trademarks of A.E.T. Europe B.V. All other product and company names are trademarks or registered trademarks of their respective owners.

## Document Information

---

**Filename:**                    **Technical White Paper BlueX**  
                                  **The Concepts of BlueX explained**

**Document ID:**            **Technical\_White\_Paper\_BlueX\_v1.1**

### Project Information:

#### Document revision history

Version	Date	Author	Changes
1.0	08-10-2004	H. Beljaars	Initial document
1.1	08-11-2004	H. Beljaars	Updated

**WE RESERVE THE RIGHT TO CHANGE SPECIFICATIONS WITHOUT NOTICE**

## Table of contents

---

<b>Warning Notice</b> .....	<b>I</b>
<b>Document Information</b> .....	<b>II</b>
<b>Table of contents</b> .....	<b>III</b>
<b>About the Product</b> .....	<b>IV</b>
<b>1 Introduction</b> .....	<b>1</b>
<b>2 Workflow</b> .....	<b>2</b>
<b>2.1 Example workflow</b> .....	<b>2</b>
<b>2.2 How can BlueX help out</b> .....	<b>3</b>
<b>2.3 BlueX example workflow</b> .....	<b>3</b>
2.3.1 Certificate Authorities .....	3
2.3.2 LDAP .....	3
2.3.3 Tokens .....	3
2.3.4 Smart card printers .....	3
2.3.5 PIN and PUK mailers .....	3
2.3.6 Example workflow .....	4
<b>3 Role based</b> .....	<b>5</b>
<b>4 BlueX Remote components</b> .....	<b>5</b>
<b>4.1 Communication between BlueX and remote components</b> .....	<b>6</b>
4.1.1 Standard BlueX remote component workflow .....	6
4.1.2 Overview of remote components .....	8
<b>5 Internal workings of BlueX</b> .....	<b>9</b>
<b>5.1 Technical viewpoint on BlueX interfaces</b> .....	<b>9</b>
<b>5.2 Business related viewpoint on BlueX interfaces</b> .....	<b>10</b>

## About the Product

---

AET's BlueX system is a Digital ID management system supporting the entire token production process within an (complex) organisational structure.

Deploying Digital IDs in an organisation can require huge costs and efforts and demands a number of issues and consequences to be taken into account. Not only may each organisation have its own infrastructure and organisational workflow in place, but such issues as printing and initialising tokens have to be considered as well. In short, the process of issuing, distributing and managing tokens demands a management system that is both flexible and easy to use and seamlessly integrates into existing company structures. This is where the BlueX system for Digital ID management comes in to help organisations solve their token deployment issues.

BlueX is designed to solve the problem of token deployment. With BlueX Digital ID management software, organisations can leverage their existing expertise and investments in infrastructure to reduce the cost and efforts of deploying tokens, irrespective of how many users are involved. BlueX provides an enterprise wide system for token production in small and large amounts. High level of system configurability allows reflecting the company's organisation structure and incorporating changes in organisation workflow almost in real time.

The BlueX system supports integration with a variety of hardware, including smart card printers and different types of smart card readers/writers. The BlueX system provides a high level of security, deploying SSL with high encryption and client certificate authentication as well as access level definition via Access Control Lists (ACL).

# 1 Introduction

Some of the parts that define an organisation are that one or more persons decided to work together as a group. Within that group there are multiple (paper) workflows and business rules that define the cooperation between the persons.

Workflows therefore are also business rules that apply to organisations. Business rules are rules that define how a digital identity is going to be used with an organisation. Examples of business rules are: has a signature set by a digital identity the same status as a handwritten signature within an organisation? How will a digital identity be deployed within the company? Checking the identity of a person prior to receiving a digital identity is also a part of a business rule. The business rules define the workflow within the organisation.

One of the possibilities to streamline organisational workflows is to introduce the concept of digital identities. A digital identity is a piece of electronic hardware or software that uniquely identifies a person in that organisation. With this digital identity persons can electronically sign, authenticate and encrypt data. Examples of how the digital identities are used in organisations are: smartcard logon, web authentication and signing of documents. This digital identity follows some of the same workflows as a real person: it gets created during hiring of a person and gets revoked during firing of that person. These, and many more, organisation workflows apply to digital identities. Some of these workflows are discussed in this paper.

A third part of digital identities are the technical requirements. Technical requirements that apply to a digital identity are: does my digital identity integrate with Microsoft Active Directory? Which Certificate Authorities can be used?

To reflect all these organisational requirements, you need an electronic identity management system that copes with all these different needs. BlueX is a workflow based identity management system that can handle all the different aspects of all the organisational needs.

## 2 Workflow

Within organisations there are multiple (paper) workflows and business rules. If we look at organisational workflows and moments that have to do with creating or revoking digital identities, those are: when people are hired, fired. In addition, when people lose or forget their digital identity.

Looking at all those workflows and moments during the hiring and firing of people, multiple departments must work together. Different departments do a combined effort to administratively 'create' a person within an organisation. One part during the administrative creation of a person with an organisation could be the creation of a digital identity. When an organisation would decide to manually create/issue digital identities all these departments have to work together to issue a digital identity. Some business rules that apply here are: what kind of permissions does this person need? Does this person need a digital identity or not? Should it be a smart card or not?

### 2.1 Example workflow

Issuing a digital identity for a person that is just hired could look like this in an organisation without BlueX.

1. On day one the newly hired person goes to Human Resources department (HR).
2. HR fills in all the details of that person in their computer system,
  - HR phones or sends e-mail to the head of the department advising him that the data is entered.
3. The next step for that person is to go to the head of his department.
  - The head of the department verifies that all data for that person in the computer system are correct, and if necessary add or changes data.
4. The person now goes to the IT-department to get his credentials.
  - The IT-department creates a user account.
  - The IT-department phones or sends an e-mail message to the department head to let him know that the person is activated within the computer system and ask him what the permissions should be.
  - The IT-department verifies that all data for that person is in the computer system, and if necessary add or changes data.
5. At this moment all the data is entered into the system and the digital identity can be produced.
  - A token or smart card has to be printed.
  - PIN and/or PUK mailers have to be produced.
  - A digital identity or identities have to be requested by one or more Certificate Authorities (CAs)
  - Digital identities have to be published into different (online) systems.
  - An accompanying letter has to be printed.

Some other workflows that relate to digital identities within organisations are:

- People who leave:
  - All digital identities have to be revoked.
- People who forget to bring their digital identity with them:
  - Temporary digital identities have to be created so that they still can work. Do any restrictions apply to this temporary digital identity?
- People who lost their digital identity:
  - Replacement of digital identities has to be created and the old digital identities have to be revoked.

## 2.2 How can BlueX help out

BlueX is a workflow-based system that can reflect any organisational administrative workflow, turning paper and phone calls into web pages. As a result of this concept BlueX can perfectly integrate within current and future organisational workflows. Instead of a paper trail in your organisation BlueX logically turns paper into an electronic workflow based on web pages. All manual steps that are taken to create digital identities BlueX can automate. For example, BlueX can create a computer account, request digital identities by different CAs of different vendors, supports multiple smart card printers and can provide security paper for PIN and PUK letter.

## 2.3 BlueX example workflow

### 2.3.1 Certificate Authorities

BlueX is integrated with all the major CAs, such as:

- Microsoft 2000 CA
- Microsoft 2003 CA
- Baltimore UniCERT CA
- Verisign CA
- RSA Keon CA
- Entrust 6.x CA
- Entrust 7.x CA

### 2.3.2 LDAP

BlueX has the possibility to publish data and create entries in all the major LDAP compliant directory applications, such as:

- Microsoft Active Directory
- BlueX can create and disable user accounts
- Any LDAP compliant directory service

### 2.3.3 Tokens

BlueX supports any token that has a PKCS #11 compliant or CSP interface, such as the AET middleware.

### 2.3.4 Smart card printers

BlueX can physically personalise a smart card by, for example, printing a name or organisational logo on a card. For this purpose BlueX has integrated an ever-increasing number of smart card printers, such as:

- Eltron smart card printer
- Dai Nippon smart card printer
- Fargo smart card printer

### 2.3.5 PIN and PUK mailers

To safely distribute PIN and PUK codes to end users, AET as developed their own security paper. Just like when you receive a new bank card, BlueX will print the PIN code of the token on security paper thereby making it impossible for other people to get a hold of the PIN code of the token. It is also possible to integrate already existing security paper into BlueX.

### 2.3.6 Example workflow

If we look at the example workflow defined above from a BlueX perspective, we could write it down in the following manner:

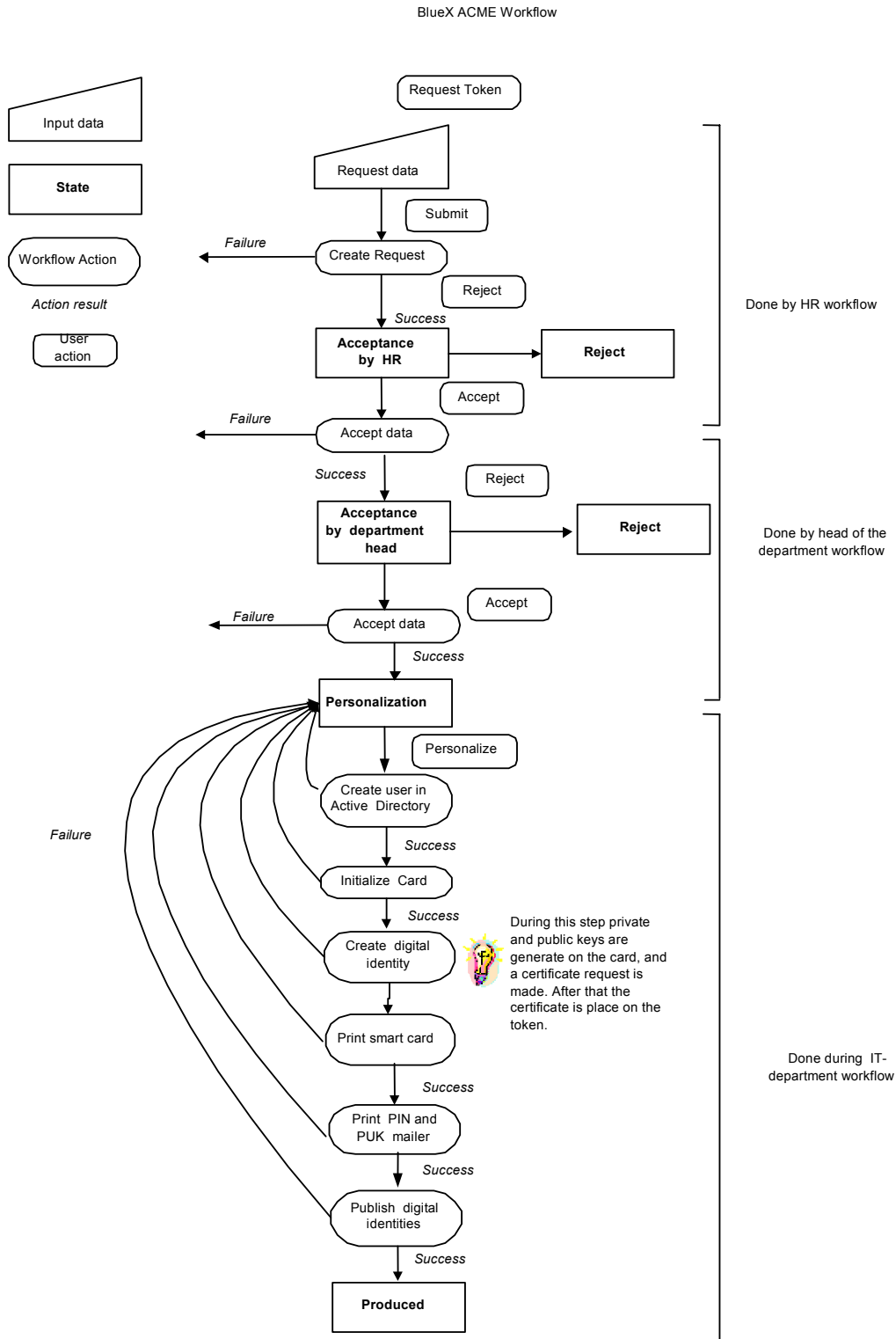


Figure 1: Example workflow

### 3 Role based

As you can see in the example above, there are multiple persons with different roles involved in collecting and verifying all the necessary data and producing a digital identity. BlueX reflects the organisational needs for role separation. This means that different roles within BlueX can do different things, but this also means that if a role does not have the permissions to do something, all these options are hidden for that user. In practise this means that users of the BlueX system can only see things they have permission for.

In the example above there are three different organisation roles to be identified: the HR department, the head of the department and IT department. A possible BlueX reflection of this organisations role separation could be the RA (Registration Authority) role for the HR department, a VA (Validation Authority) for the head of the department and a PA (Production Authority) role for the IT-department. The RA is primarily responsible for the enrolment of the data, a VA validates the information entered into BlueX by the RA, and the PA produces the digital identity. It is – of course – possible to reflect any other organisation role separation into BlueX

### 4 BlueX Remote components

One of the problems that a digital identity management system faces is the fact that different components/applications or data sources that are required during the production of a digital identity are physically or network topologically located in a different site. Most of the times those sites are protected by a firewall. As a result of this it is not possible for BlueX to directly contact those different components/applications, but components/applications can connect to the resources that are outside their site.

To resolve this problem BlueX introduces a new concept called 'BlueX remote components'. A BlueX remote component is a small application that is installed on-site and can connect to the component/applications or data source. A remote component acts as a proxy of BlueX and can be located at a remote site behind a firewall that does not allow incoming connections. The remote component uses the same method of connecting as a normal secure web connection for a browser.

This BlueX remote component actively connects to the BlueX applications server to see whether or not there is work for that component, and acts like some sort of proxy server between the BlueX applications server and the component/application or data source.

During the processing of the workflow, tasks that should be carried out by the different remote component are set ready for retrieval by the BlueX application server. If there is a task to do for that BlueX remote component it deals with that and reports back to the BlueX application server of what the result was of that task.

As a result of this concept it is possible that you can use a CA that is protected from the outside by a firewall. This is a normal situation in an environment that uses not the organisational CA but a third party CA. In the extreme case it is possible to use components/applications and data source that are all distributed over the Internet (see figure 2).

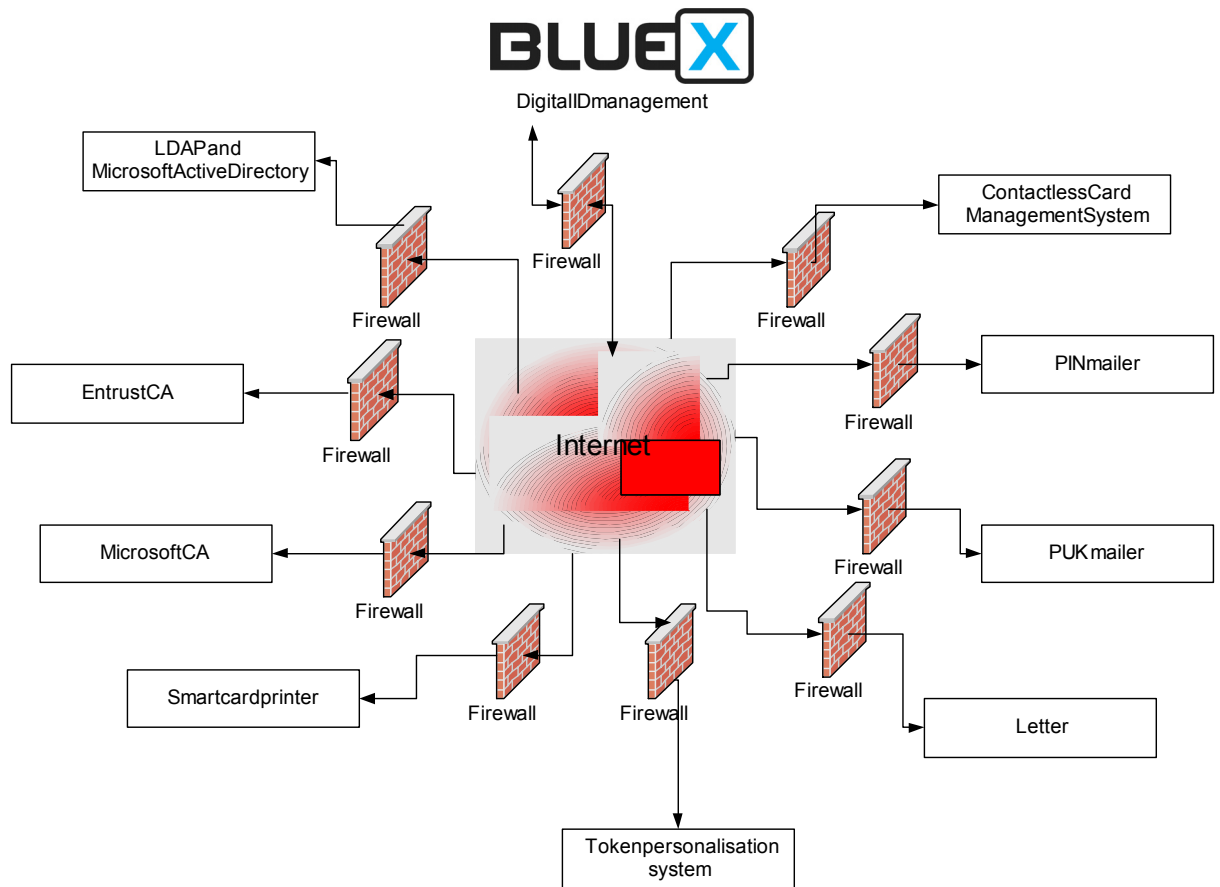


Figure 2: BlueX remote components

## 4.1 Communication between BlueX and remote components

The BlueX remote components communicate via standardized methods to the BlueX application server.

### 4.1.1 Standard BlueX remote component workflow

This remote communication protocol can be broken-down in several steps.

**Step 1:**

BlueX remote component starts.

**Step 2:**

BlueX remote component connects to the BlueX application server.

**Step 3:**

BlueX remote component authenticates itself to the BlueX application server. The authentication to the BlueX application server is certificate based. Every remote component has its own certificate that can be used to authenticate. Since the BlueX application server knows which certificate belongs to which remote component, it can identify these components. The certificates that are used by the BlueX remote components can be located on a token or can be in software. The DN of the certificates identifies the remote component.

**Step 4:**

During the authentication process the BlueX application server grants access or denies access to the remote component.

**Step 5:**

If the authentication was successful an SSLv3 session is setup between the application server and the remote component.

**Step 6:**

The remote component checks on the BlueX application server whether or not there is a task that needs to be performed. If that is the case the remote component retrieves the necessary information from the application server, and performs the task.

**Step 7:**

After the task is completed the remote components reports back to the application server what the result of the task were. The task could have succeeded, failed or in that same process data can be send back.

In figure 3 the remote component workflow is described:

\* Client connects to BlueX application server to see whether or not there is a task to be performed.

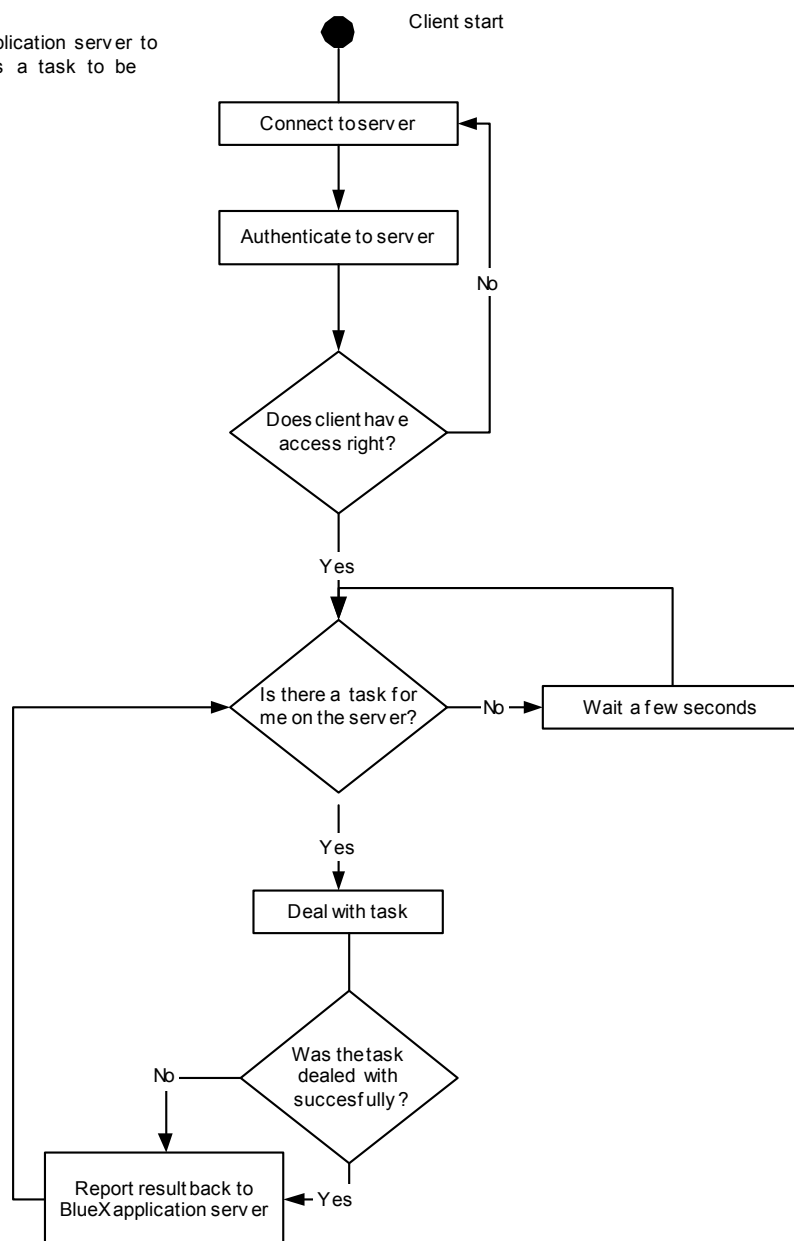


Figure 3: Remote component workflow

### 4.1.2 Overview of remote components

Looking at how a BlueX remote CA component is setup as an example for how BlueX remote components work, there are several applications to be identified: the CA, the BlueX remote component and the BlueX application server. The BlueX remote CA component communicates to the CA with the interfaces that are available for that CA. For the Microsoft CA those are the Microsoft COM components called 'smartcard enrolment control' for the smart card enrolment and the Microsoft COM interface 'Icertadmin' for revoking certificates. Other CAs have different interfaces. For example the BlueX remote component uses the ARM interface to communicate to the UniCERT Baltimore CA. Entrust provided multiple interfaces that BlueX can use, for example the 'Entrust Admin toolkit or Entrust file toolkit'.

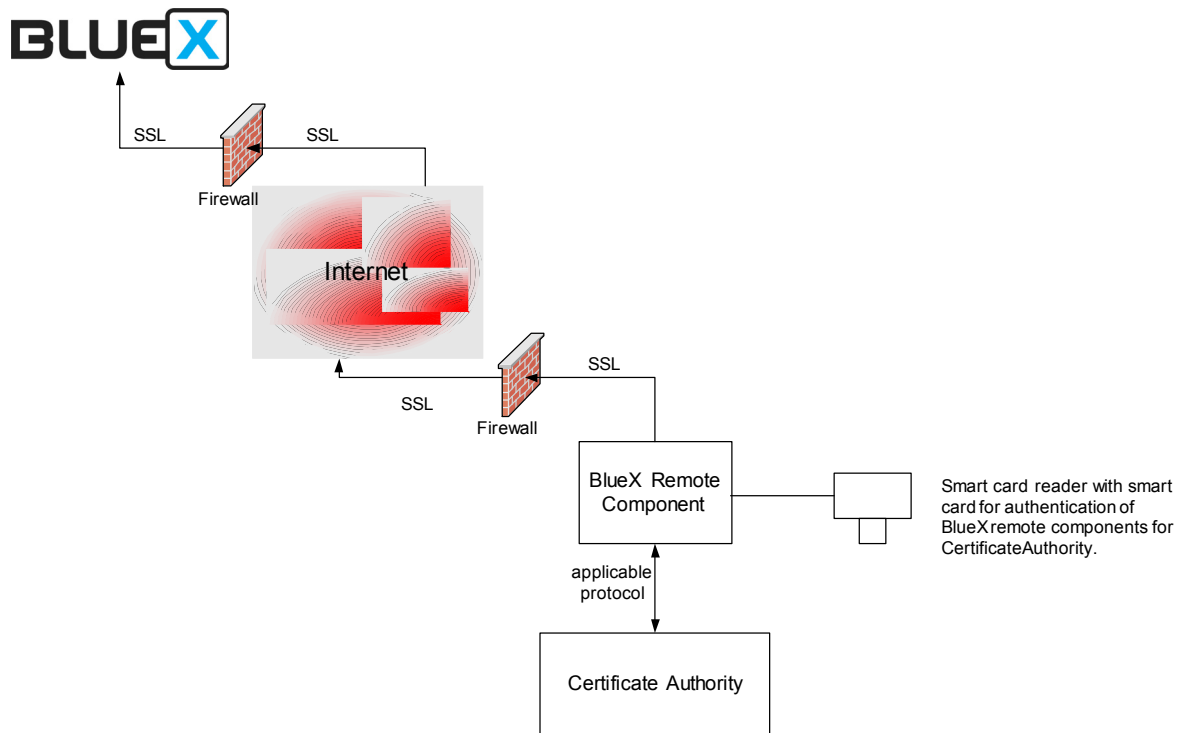


Figure 4: Remote CA component configuration

## 5 Internal workings of BlueX

One of the issues organisations have to address during the deployment of digital identities is the issue regarding the ownership of data. What that means is, when you introduce a system that uses different data sources for collecting information, you create a system that also has (partial) information stored. The issue now is that who manages the data? Is that BlueX or the original system? To resolve this issue BlueX can operate in two extremely different modes, and everything in between. Taking the two different modes into extreme: mode 1: BlueX is responsible for all the data. Mode 2: BlueX is not responsible for any data.

Mode 1 gives the possibility to manage all data from BlueX. This means that BlueX manages and manipulates all data. In mode 2 BlueX is a part of a different system, and that other system is responsible for managing data.

If other applications or BlueX remote clients want to access the BlueX application server they could use several interfaces.

### 5.1 Technical viewpoint on BlueX interfaces

After a client (BlueX or otherwise) has successfully authenticated itself towards the application server it can access BlueX. There are three different interfaces towards BlueX: 1. The user/ HTML interface (for example a web browser would use this to interact with BlueX). 2. The RCCP interface. This is the interface used by the remote components to interact with the application server. 3. An XML interface. This can be used by third party applications to interface to BlueX. Everything that can be done using the user / HTML interface can be done with the use of this XML interface. For example, if in interface 1 an user presses a button, this is in fact a XML command.

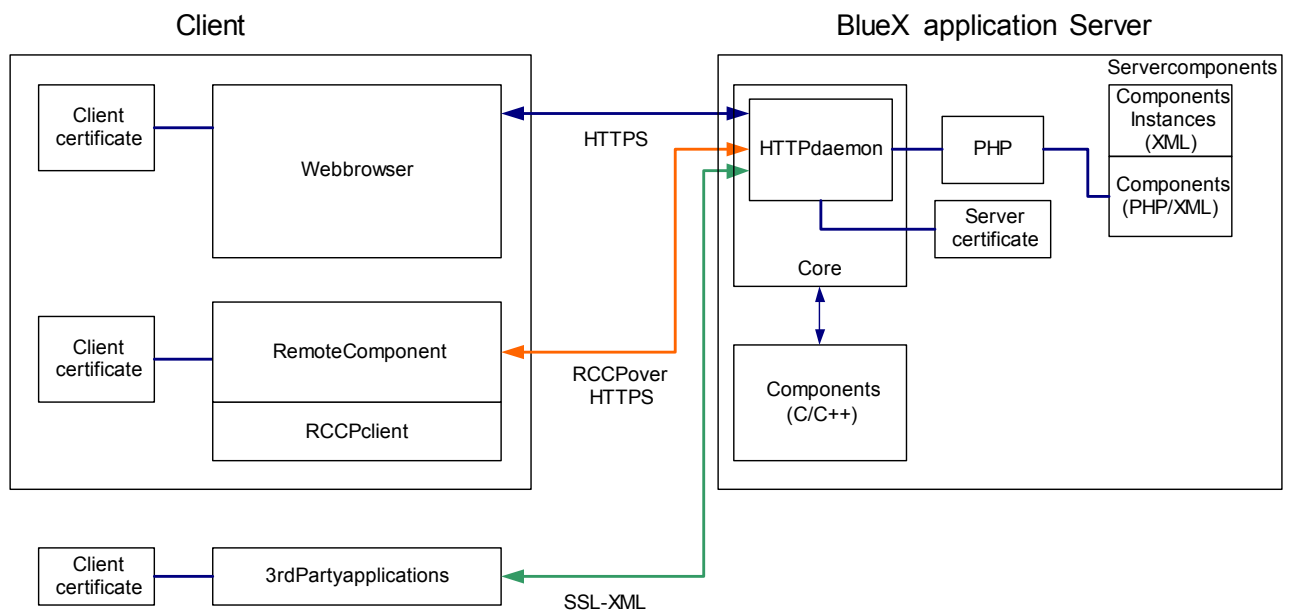


Figure 5: technical view on BlueX

## 5.2 Business related viewpoint on BlueX interfaces

BlueX uses a generic framework combined with open standards to abstract itself from all proprietary technologies. As a result of this concept BlueX is hardware and software independent.

To integrate BlueX within any organisation it has a multiple abstractions layer that can reflect any organisational business rule and workflow. The modular approach of the remote component framework makes it possible to add support for new hard -and software devices easily.

Looking at the BlueX application server from a business point of view, there are three different main components to be identified: business rules, remote component framework and the workflow. The external interface is connected to the business rule component. The business rule component 'translates' all actions from given to the external interface into actions that can be dealt with internally. An action coming from the external interface could be 'produce PIN letter'. In this case the business rule component decides whether or not this action may be done by that particular external application, and if that is the case it will interact this with the workflow component. The business rule component interacts with both the remote component framework as with the workflow component. The remote component framework translates actions request from the business rule component into tasks that can be dealt with by remote component. It uses a specific interface to talk to all the different remote components. In the case of producing a PIN letter it will interact with the PIN letter interface and produces a task for a remote PIN letter component. The workflow component coordinates the workflow of all the different actions that requests from the business rule component. In the example of producing the PIN letter it will coordinate what must be done to produce a PIN letter and takes initiative to gather all the required information.

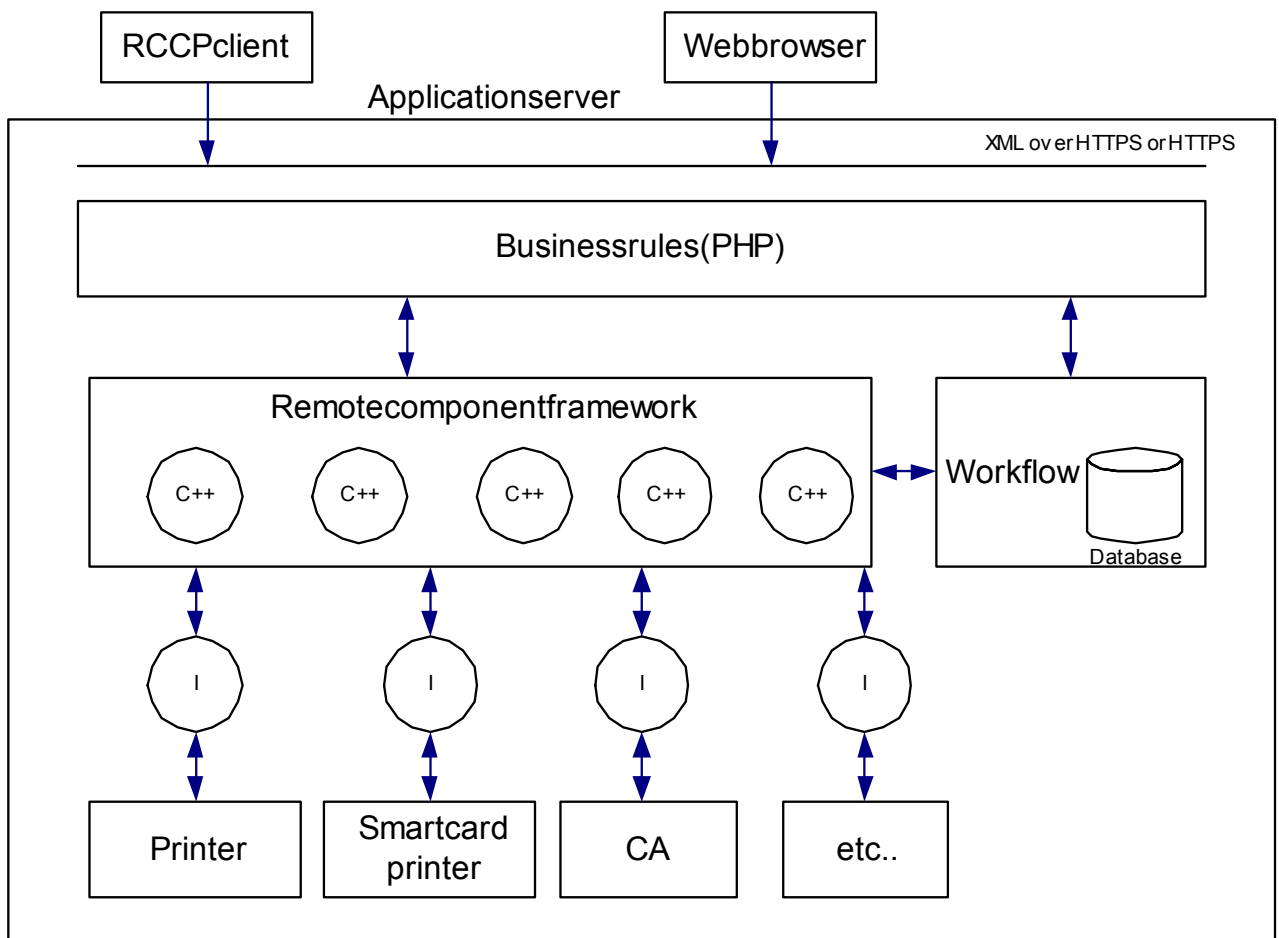


Figure 6: business view on BlueX