MI51
Signature et envoi de documents électroniques au format PDF

Alexandre Belloni

Introduction

Aide à l'Utilisateur de Documents Électroniques

Introduction

Aide à l'Utilisateur de Documents Électroniques

- transforme et regroupe les fichiers habituels (au format Word et Excel) en fichiers au format PDF

Introduction

Aide à l'Utilisateur de Documents Électroniques

- transforme et regroupe les fichiers habituels (au format Word et Excel) en fichiers au format PDF
- maîtrise l'envoi des documents électroniques

Introduction

Aide à l'Utilisateur de Documents Électroniques

- transforme et regroupe les fichiers habituels (au format Word et Excel) en fichiers au format PDF
- maîtrise l'envoi des documents électroniques
- signe les documents avant l'envoi au client

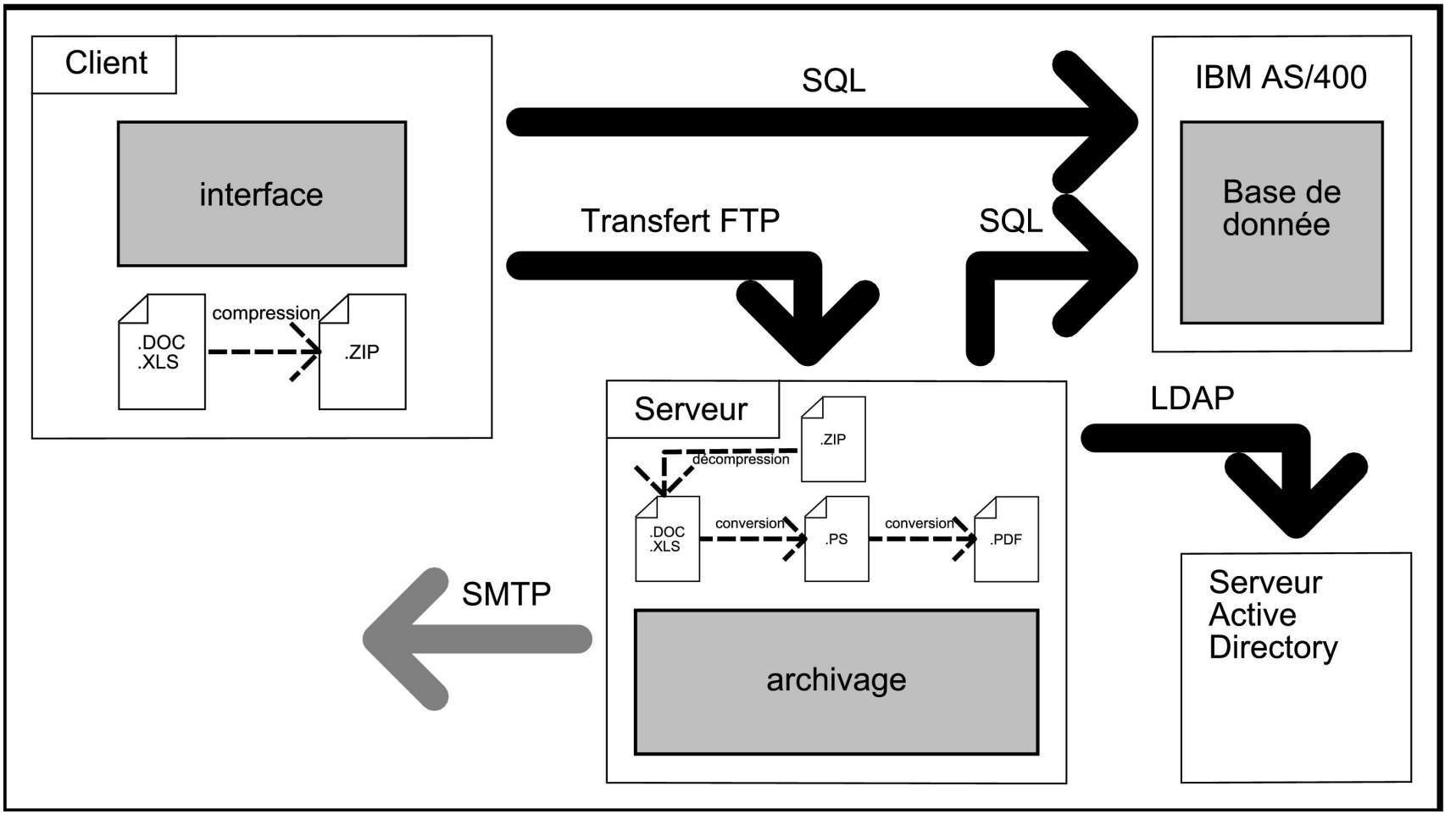
Introduction

Aide à l'Utilisateur de Documents Électroniques

- transforme et regroupe les fichiers habituels (au format Word et Excel) en fichiers au format PDF
- maîtrise l'envoi des documents électroniques
- signe les documents avant l'envoi au client
- utilise les standards OpenPGP, S/MIME

Introduction

Aude - Architecture



Analyse d'un mail

Delivered-To: alex@piout.net
Received: from portail1.utbm.fr (portail1.utbm.fr [193.48.246.2]) by lilith.piout.net (Postfix) with ESMTP id D3401182352 for <alex@piout.net>; Sun, 9 May 2004 14:36:04 +0200 (CEST)
[...]
Received: from portail1.utbm.fr (localhost [127.0.0.1]) by hera.utbm.fr (8.9.1a/jtpda-5.3.1) with ESMTP id MAA29536; Sun, 9 May 2004 12:18:55 +0200 (MEST)
Received: from vers-webmail.utbm.fr (localhost.localdomain [127.0.0.1]) by portail1.utbm.fr (8.12.8/jtpda-5.4) with ESMTP id i49AIsPA028659 for <etudiants@utbm.fr>; Sun, 9 May 2004 12:18:55 +0200
Received: by vers-webmail.utbm.fr (Postfix, from userid 48) id EE112802E; Sun, 9 May 2004 12:18:53 +0200 (CEST)
Received: from d213-101-193-87.cust.tele2.fr (d213-101-193-87.cust.tele2.fr [213.101.193.87]) by webmail.utbm.fr (IMP) with HTTP for <ccholez@localhost.localdomain>; Sun, 9 May 2004 12:18:53 +0200

Analyse d'un mail

Message-ID: <1084097933.409e058dddbfe@webmail.utbm.fr>
Date: Sun, 9 May 2004 12:18:53 +0200
From: "Caroline.Cholez@UTBM.fr" <Caroline.Cholez@utbm.fr>
To: etudiants@utbm.fr
Subject: PROMO03 Tee shirt!!!! important
MIME-Version: 1.0
Content-Type: multipart/mixed;
boundary="-MOQ10840979330cc776d4010a6847c032b72b9340d616"
User-Agent: Internet Messaging Program (IMP) 3.2.2
X-Spam-Status: No, hits=1.3 required=6.0
tests=LINES_OF_YELLING,PLING_PLING autolearn=no
version=2.63
X-Spam-Level: Score:*
X-Spam-Checker-Version: SpamAssassin 2.63 (2004-01-11) on
portail1.utbm.fr
Content-Transfer-Encoding: 8bit
X-Validation-by: ae@utbm.fr
Content-Length: 127594

Analyse d’un mail

```
This message is in MIME format.
—MOQ10840979330cc776d4010a6847c032b72b9340d616
Content-Type:  text/plain; charset=ISO-8859-1
Content-Transfer-Encoding:  8bit
Salut les gens
Pour ceux de la promo qui n’auraient pas encore remarqué, nous
n’avons toujours pas de tee shirt!!!!!
[...]
—MOQ10840979330cc776d4010a6847c032b72b9340d616
Content-Type:  application/x-zip-compressed; name="voter1.zip"
Content-Transfer-Encoding:  base64
Content-Disposition:  attachment; filename="voter1.zip"
UEsDBBQAAAAIAAhWqTBEVl3VG2MAAACsAAAKAAAAdm90ZXIxLmRvY+xYeTzU39f/zDQxso1
oiwhy9iXaEPWImRLiSR7QpR9CYVUtiR7SLZihhKFSIws2fdd1ixjnjuW59uj7/P0e/3++/6
c+4599wz537ueeeej8/1NN2JuUw90DbIQDugNQIZRPKTDAba2S0GBUFam7I1AoFAFGmARvi
```

S/MIME

S/MIME

- Extension de MIME

S/MIME

- Extension de MIME
- Défini de nouveaux types

S/MIME

- Extension de MIME
- Défini de nouveaux types
- Utilise les principes de cryptographie asymétrique, cruptographie symétrique, hachage.

Hachage

Hachage

- Une fonction de hachage produit un condensé des données.

Hachage

- Une fonction de hachage produit un condensé des données.
- Le condensé caractérise de manière quasi-unique un texte ou des données.

Hachage

- Une fonction de hachage produit un condensé des données.
- Le condensé caractérise de manière quasi-unique un texte ou des données.
- Cela permet de réduire la taille des données à traiter par les fonctions de cryptage.

SHA-1

Le condensé SHA-1 de la chaîne “Ce message sera signé” est 4ab6012af0b621377e35f44198ab5fa6a10c8a51

SHA-1 fourni un nombre de 160 bits.

Pour en savoir plus : http://www.itl.nist.gov/fipspubs/fip180-1.htm

Comment signer ?

Comment signer ?

- On construit le corps du mail avec toutes les parties MIME.

Comment signer ?

- On construit le corps du mail avec toutes les parties MIME.
- On caclule le condensé du corps du mail.

Comment signer ?

- On construit le corps du mail avec toutes les parties MIME.
- On caclule le condensé du corps du mail.
- On signe le condensé et on le rajoute en S/MIME.

Comment signer ?

- On construit le corps du mail avec toutes les parties MIME.
- On caclule le condensé du corps du mail.
- On signe le condensé et on le rajoute en S/MIME.
- On ajoute les entêtes.

Un mail signé

```
This is an S/MIME signed message

----E95DB8E1D894FC5EF338EA84F0F40006
Content-Type:  text/plain

Ce message sera signé

----E95DB8E1D894FC5EF338EA84F0F40006
Content-Type:  application/x-pkcs7-signature; name="smime.p7s"
Content-Transfer-Encoding:  base64
Content-Disposition:  attachment; filename="smime.p7s"

MIIExwYJKoZIhvcNAQcCoIIEuDCCBLQCAQExCzAJBgUrDgMCGgUAMAsGCSqGSIb3
DQEHAaCCApswggKXMIICAAIBADANBgkqhkiG9w0BAQQFADCBkzELMAkGA1UEBhMC
RlIxHjAcBgNVBAgTFVRlcnJpdG9pcmUgZGUgQmVsZm9ydDEQMA4GA1UEBxMHQmVs
```

Comment vérifier ?

Comment vérifier ?

- On calcule le condensé du corps du mail.

Comment vérifier ?

- On calcule le condensé du corps du mail.
- On récupère la clé publique de l'expéditeur si nécessaire

Comment vérifier ?

- On calcule le condensé du corps du mail.
- On récupère la clé publique de l'expéditeur si nécessaire
- On vérifie la signature

Les PKI

Ou comment récupérer de façon sécurisée les clés publiques

Les PKI

Ou comment récupérer de façon sécurisée les clés publiques

- Remise en main propre

Les PKI

Ou comment récupérer de façon sécurisée les clés publiques

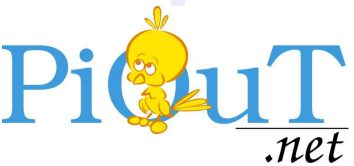
- Remise en main propre
- Les Certificate Authority (CA - Autorités de certification)

Les PKI

Ou comment récupérer de façon sécurisée les clés publiques

- Remise en main propre
- Les Certificate Authority (CA - Autorités de certification)
- Les réseaux de confiance

Pour en savoir plus



Pour en savoir plus

- The Internet Engineering Task Force :
  http://www.ietf.org/

Pour en savoir plus

- The Internet Engineering Task Force : http://www.ietf.org/
- MISC 13

Pour en savoir plus

- The Internet Engineering Task Force : http://www.ietf.org/
- MISC 13
- www.gnupg.org

Des questions ?