EU-MIDT

Card Issuing and Networking Committee

EU-MIDT/CINC/003-2010

Technical details for the settings and use of the Message Box tool for Card Issuing Authorities to securely exchange information (through the CORTE website)

PREPARED BY: Cédric Desmet (EWAPPS)
DATE: 04/02/2010
EU-MIDT CINC–003-2010

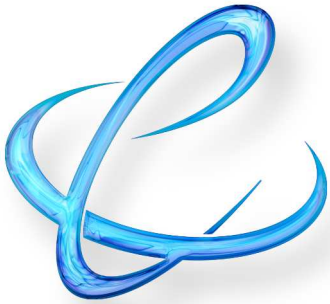
REF : EU-MIDT/CINC/003-2010

EU-MIDT SECRETARIAT DOCUMENT PREPARATION

OPERATION	NAME	ORGANISATION	DATE
PREPARED BY	Cédric DESMET	EWAPPS	04/02/2010
CHECKED BY	Christoph BAIER Armand BIBERICH Herman GROOTERS Marja VAN DER WEL Henk-Jan VAN DER MOLEN Birgit SÄÄV	Switzerland Luxembourg The Netherlands The Netherlands The Netherlands Sweden	10/02/2010
APPROVED BY	Rémy RUSSOTTO	CORTE	10/02/2010
ISSUED BY	Secretariat	CORTE - MIDT	26/03/2010

CHANGE CONTROL LIST

VERSION	DATE	NAME	DESCRIPTION



Ewapps
www.ewapps.com

MIDT

Secure messaging platform

Ewapps s.a.
496, Avenue Brugmann
B-1180 Brussels
Belgium

T.V.A. : BE 465.407.582
BBL : 310-1338905-03

Contact
Desmet Cédric
Tél.: +32-(0)2-481.59.30
Direct: +32-(0)2-481.59.33
Fax: +32-(0)2-481.59.31
E-mail: c.desmet@ewapps.com
Web: www.ewapps.com

1. Project description

Purpose of this project is to use the MIDT website as a secure messaging platform allowing card issuing authorities to communicate together.

Communication between the national authorities will always be one on one communication.

The “deadline” for this project has been settled on : end February 2010.

A lot of screenshots would be realized and submitted to have a first feedback on the application.

The testing period will begin on mid march 2010 with 5 National Authorities.

2. Functionalities

2.1. Access levels

2.1.1. Experts and Supervisor access

Experts are always member of one (and only one) member state.

Each expert will have access to his own private area and to a messaging platform using a login (= email address) and password.

A link to the private area will be added to www.corte.be menu.

After being identified, experts will be able to:

- Access to private information ;
- Access to a messaging exchange platform. Access to this platform will be granted by member states supervisors.

2.1.2. Manage accounts for the exchange platform

Member state supervisor (National Authority supervisor)

Each member state will receive a supervisor login to manage (create, modify and delete) experts related to his country.

National Authority must nominate at least one person to manage those functionalities.

Supervisor will be able to:

- Manage (create, modify and delete) others supervisors for his own National Authority
- Manage (create, modify and delete) Experts related to his National Authority.

Supervisor of each National Authority will be created by the MIDT Administrator. Supervisor will receive his password by email or by post.

Member state user (National Authority Expert)

Member states users will be created by National Authority Supervisors.

After receiving a personal username (email address) and password, Member states users will have access to the messaging platform.

MIDT Administrator

MIDT Administrator will be able to manage:

- Member states supervisors access (possibility to have more than one supervisor by National Authority) ;
- Member states users' access.

2.2. Private area : messaging platform functionalities

2.2.1.Messaging box

Only member state supervisors and nominated users will get access to this website private area after logging in with the right password.

One messaging box will be linked to one member state.

Nominated users will be able to:

- Ask a question (= send a message) to another specific member state ;
- Read and delete messages in the Messaging box ;
- Reply to a message.

The Messaging box will consist of:

- An inbox containing all new incoming messages ;
- Sent Items containing messages sent to other member states ;
- Deleted Items containing messages deleted by a user and not yet deleted by the system after a defined period of time (90 days).

2.2.2.Create a new message

All member states users and supervisors will be able to send new messages.

Communication is a one to one communication between 2 member states.
National Authority will be able to send a message to herself.

The message structure will be just like an email:

- **To** (a drop down list of the registered member states registered in the system - only 1 national authority can be selected) ;
- **Subject** ;

- **Content of the message** ;
- **File attachment**.

2.2.3.New messages notification

When a member state receives a new message, all his registered users will receive an automatic email notification on their real email address.

Member state supervisor can manage how notifications will be sent to the registered users:

- One notification for each new incoming message ;
- One notification per day if there's still unread messages ;

2.2.4. Manage the Inbox

All registered users will be able to answer to a question (message).

Status of the message will also be displayed:

- Read / not read ;
- Replied / not replied

Message status will be interesting for others member state users. They don't need to read a message if another user from his member state has already answered the question.

2.2.5.Reply to a message

All member states users and supervisors will be able to reply to a new message.

When a member state user reply to a message, status of this message will automatically change for all member state users.

2.2.6.Manage Folders

All member states users and supervisors will be able to manage (create, modify and delete) folders in the messaging box.

2.2.7.General Settings

MIDT administrators will be able to define a storage limit for each member state messaging box.

MIDT administrators, member states supervisors and users will see messaging box status (total space, used space and free space).

A notification will be sent by email on the supervisor and the users of the National Authority to prevent them that they have reach the storage limit of the mailbox.

If the storage limit has been reached, the National Authority will be able to receive de new incoming messages but will not be able to respond to them. Each correspondent will receive

an email to prevent him that the volume storage of the mailbox of the contacted National Authority has been reached.

2.3. Security settings

General:

- MIDT website and the messaging platform language will be in English only ;
- Each National Authority will see his local time on the application ;
- Session time-outs will be defined. After 15 minutes, inactive users will have to enter their login and password again to get access to the private area ;
- All data will be stored in a SQL Database ;
- All messages and attachments will be encrypted in the SQL database ;
- A check must be done by an antivirus before to attach a file in a message ;
- An instruction must be send to the IT administrator of each National Authority so each National Authority will be able to connect to the secured application.

Security:

SSL Certification

- Fully validated by a valid Certification Authorities ;
- Up to 256-bit encryption (we recommend 128 bit for faster db access) ;
- 99% browser recognition.

Antivirus

- A test has been done on our server with “McAfee Virus Scan Enterprise” when we upload a file. The antivirus checks the file and deletes the file if it a virus has been found.
- The choice of the antivirus will be associated with your choice of the hosting solution.

The current technical details prescribe these steps when M&A are stored in the SQL database:

1. Using a browser, a user logs in at the CORTE message box site and types in / uploads a message and attachment (M&A);
2. The M&A are received by the CORTE web server, without passing an Anti Virus check (due to the https end-to-end encryption of the internet communication);
3. The CORTE web server places the M&A in a temporary folder;
4. The Anti Virus software scans in real time the M&A and if malware is found, it will delete M&A.
5. The M&A which passed the Anti Virus check are stored encrypted in the SQL database.

When a logged-in user wants to view an incoming message, these steps are currently prescribed:

- M&A are retrieved from the database, decrypted and passed on to the web server;

- With the M&A, the web server builds a html page for the user to download in the browser.

Encryption method

- We will use a reversible encryption algorithm to encrypt the content of the exchanged messages. The encryption method will be based on 3DES. The data will be encrypted in the database and will be decrypted to be displayed on the Inbox webpages.

Accounts and passwords:

- Actual passwords length will be increased and a minimum length will be enforced.
- Combination of numeric and alphanumeric characters will be enforced for passwords.
- Passwords will be encrypted in the database ;
- Password will have an expiration date: it must be changed by users at least each 90 days. Users will be forced to change their password at the next login.
- Reuse old passwords will no more be allowed. It will be checked and rejected if needed.
- After 10 unsuccessful trials to log on, the user account will be deactivated ;
- An inactive user will receive a notification after 90 days and his account will be deactivated ;
- Deactivated accounts will have to be reset by MIDT administrator or by the member state supervisor ;
- No account will be deleted but just deactivated so it can be reactivated easily ;
- All users can change their own password at any times ;
- If a user lost his password, he can ask the system to receive directly a new password by email (registered email address) or later by post ;

Messaging Box:

All messages will be automatically deleted 90 days after the message has been read by a user.

If a message has not been read after 90 days, member state supervisors and MIDT administrators will receive an email notification. 10 days later, the message will be deleted if it's still unread.

All the messages that have been deleted (after 90 days) will no more appear on the application but all the messages will be stored in an independent database.

Backup:

Backup planning will remain the same as MIDT website:

- One full backup every week ;
- Differential backups every days of the week ;
- 2 full backup always available.

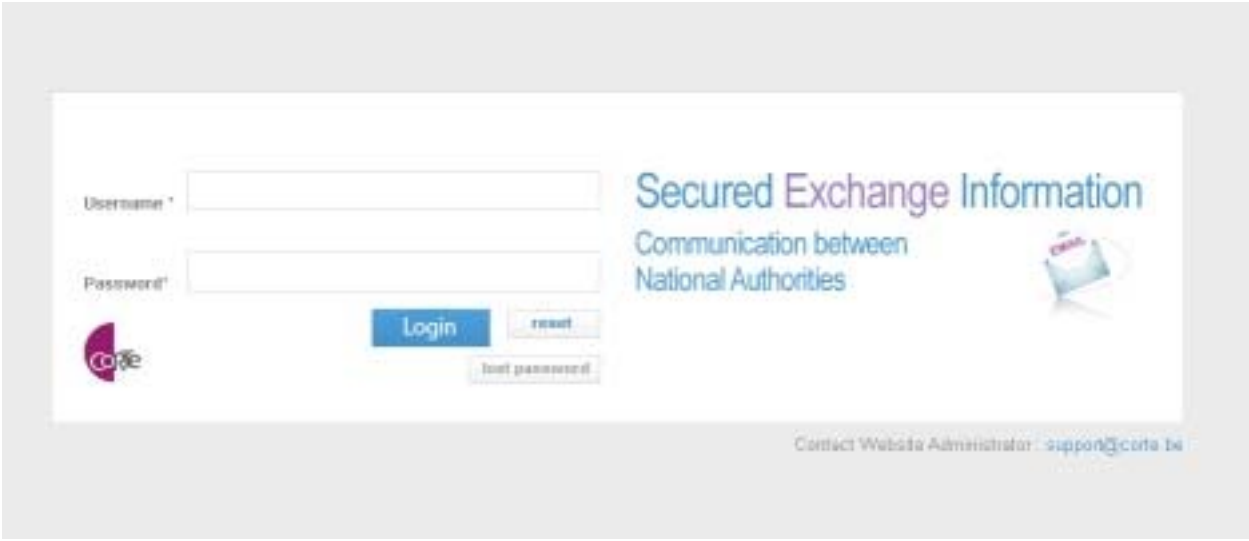
A text on the website will prevent the users that a lot of backups are done to avoid to lose data. Data can be lost only for one day.

Hosting Solution:

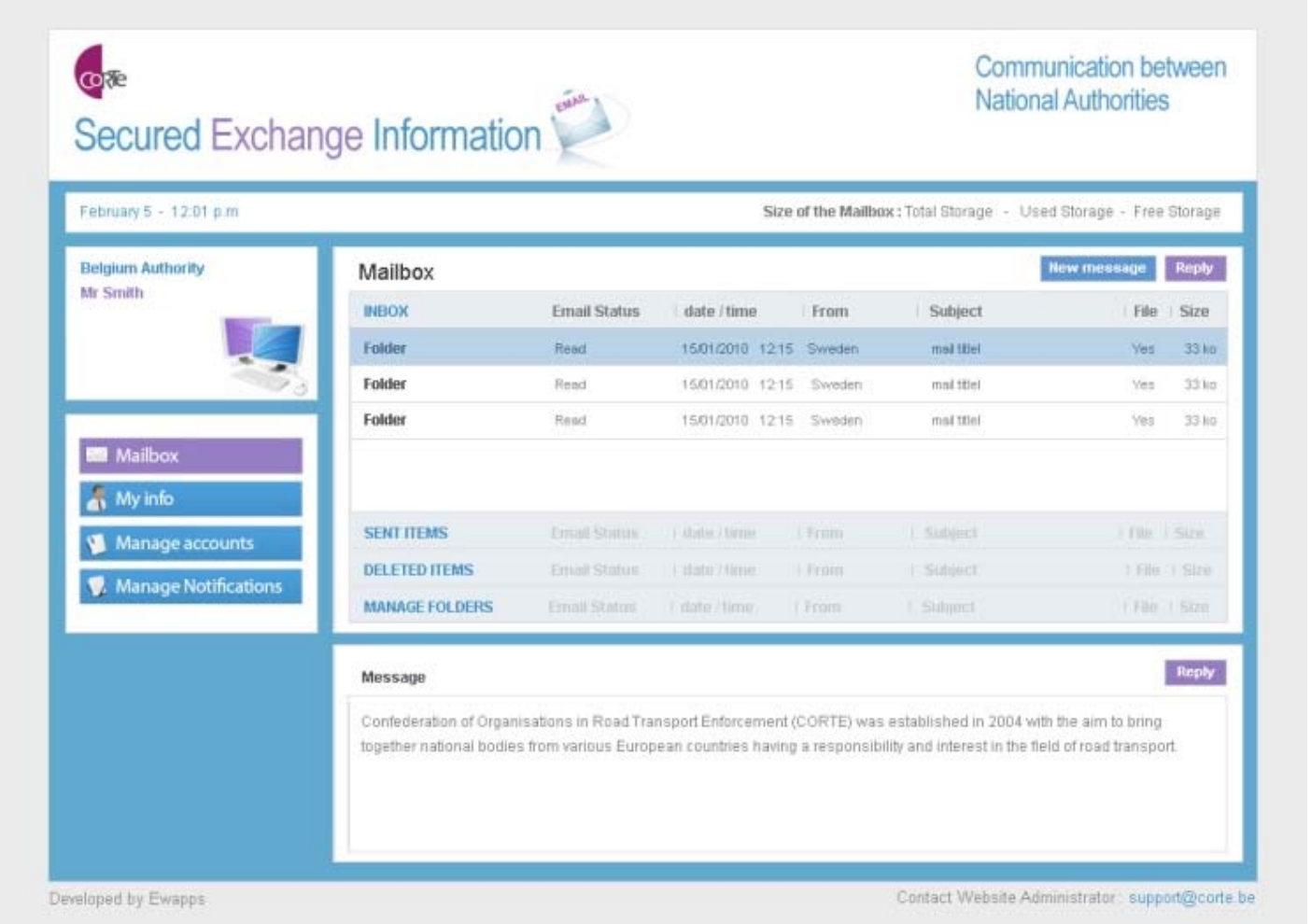
- Integration of a new SSL Certificate : encrypt communication between users and the messaging platform
- A virtual dedicated web server will replace the actual shared web server.

ANNEXE 2 : SCREENSHOTS DE L'APPLICATION

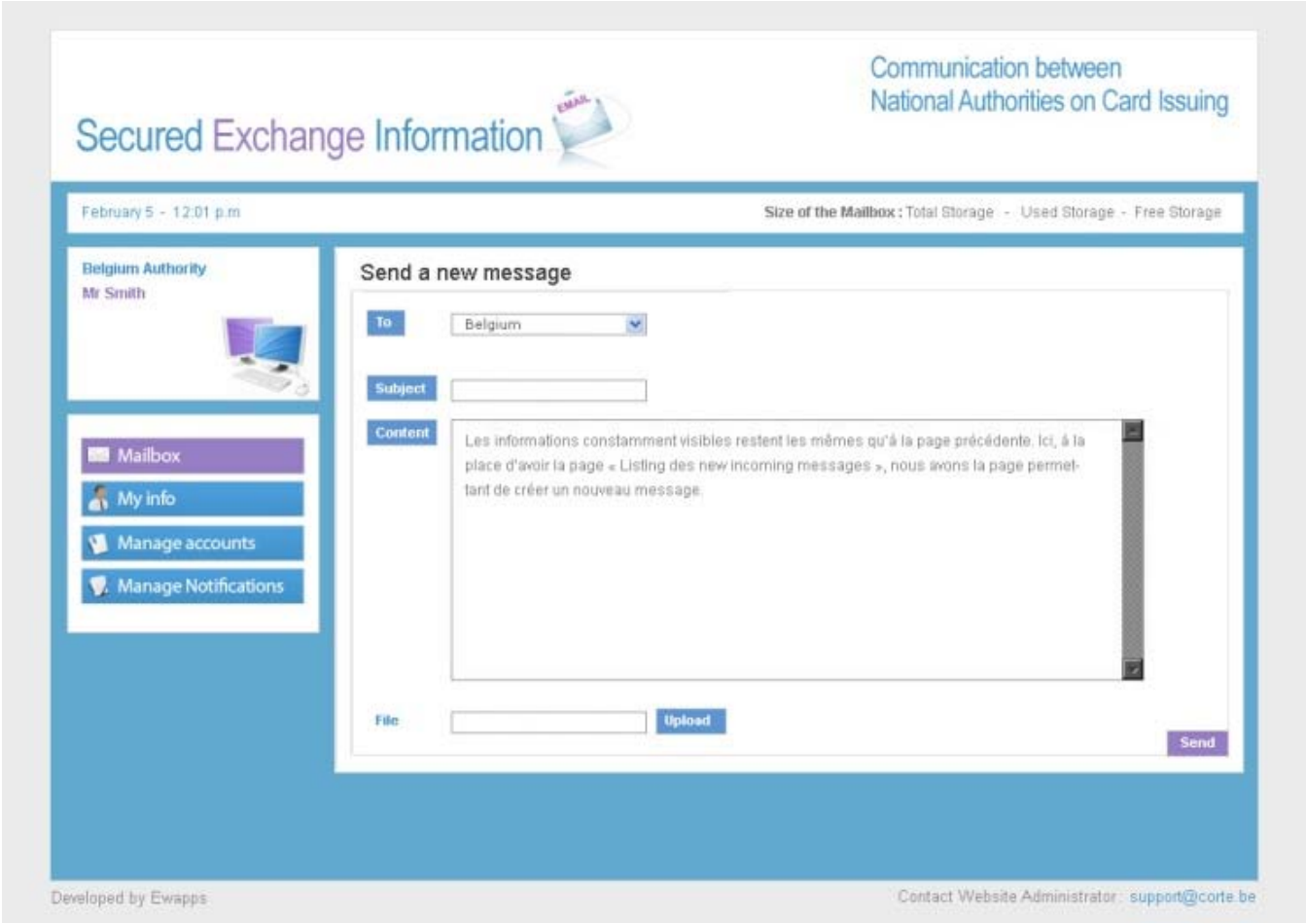
First Page : Login access



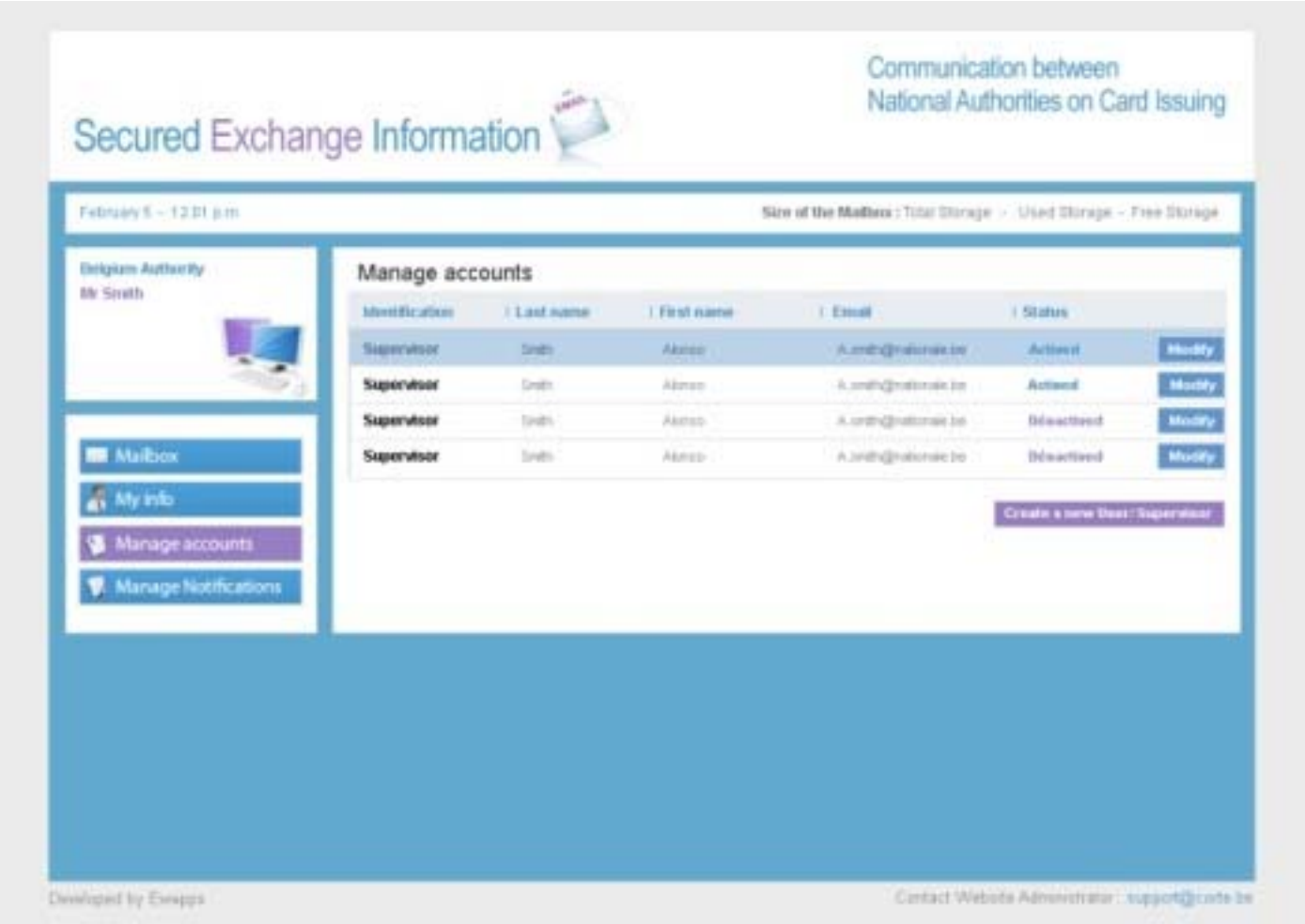
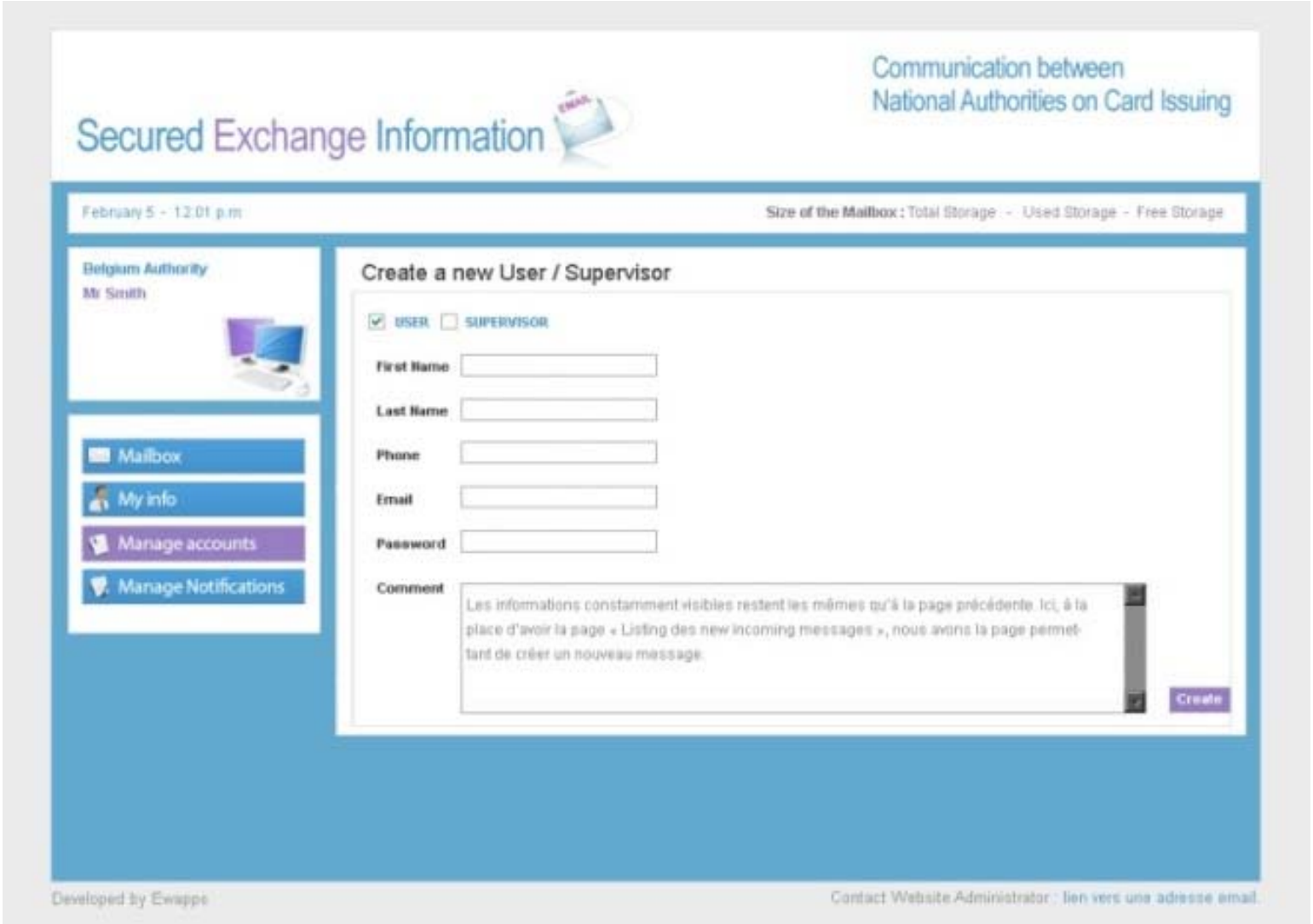
INBOX – Inbox view



INBOX – Create a new message



SUPERVISOR – Manage accounts



SUPERVISOR – Create User or other Supervisor