

eCCW Service

Technical overview

LCH.Clearnet
Version 1.0
Date : 26 June 2007

Contents

1	Introduction	3
2	eCCW Users Architecture Overview	4
2.2	Current CCW Architecture	4
2.3	Future eCCW Options	4
2.3.1	Internet based eCCW	5
	Figure 1	5
2.3.2	eCCW over MSA	5
2.3.3	eCCW over Dedicated Access	6
3	eCCW Services	8
3.1	Mains principles:	8
3.1.1	eCCW Members Security Administrators (EMSA):	8
3.1.2	eCCW access card authentication:	8
3.1.3	eCCW package includes:	8
3.1.4	Profile options:	8
4	User general Information of a eCCW access card	9
4.1	4.1 Mains principles :	9
4.2	eCCW access card picture	10

1 Introduction

The aim of this document is to provide users with a general view of the suggested solution and to facilitate members' choice.

The eCCW project is to replace the current LCH.Clearnet workstation (CCW) by a more flexible and less expensive solution.

The scope of this solution is the following:

- To create a simple client solution via internet and over private network including:
 - o A different URL for Test and Production platforms
 - o A different page for Cash and Derivatives Markets
 - o Access control through Secur ID technology

This document describes the technical architecture options and the general information of the SecurID technology.

2 eCCW Users Architecture Overview

In order to enforce system resiliency, LCH.Clearnet SA recommends to users to set up a resilient network infrastructure, compliant with their business continuity needs.

- **Recommended Workstation Configuration**

PC capable of properly running Windows XP (or above) or Linux as operating system, with an internet browser (Internet Explorer 6.0 or Firefox 2.0).

The system should be configured to allow HTTPS connexions and local execution of JavaScript programs by the web browser.

2.1 Current CCW Architecture

Currently, there are two CCW types of services offered by LCH.Clearnet:

- - CCW over a dedicated access: Consists of a dedicated access router connected to a 64 Kbps leased line. The maximum number of CCW on such architecture is three.
- - CCW over MSA: Consist of a single or redundant MSA architecture including the MSA router and switch over a leased line or a redundant leased line which bandwidth can reach 2 Mbps. To be noted that CCW over MSA is shared with CAP/MAP. In this architecture logical channels are created and each 64 Kbps channel can support three CCW. This architecture includes now (since the X Diff project such architecture includes now a single clearing channel that encompasses all clearing flows)

2.2 Future eCCW Options

With the new eCCW, the users will have several choices to implement the eCCW product:

- - Internet-based eCCW
- - eCCW over MSA (Customer private LAN)
- - eCCW over MSA (LCH.Clearnet public LAN)
- - eCCW over dedicated access (Customer private LAN)
- - eCCW over dedicated access (LCH.Clearnet public LAN)

The only difference between the MSA and the dedicated access is that dedicated access is limited to the bandwidth of your leased line (i.e. 64 Kbps in most of the cases)

Each eCCW architecture option is described below along with technical characteristics, limitations and constraints.

2.2.1 Internet based eCCW

- Characteristics (See Figure 1)
 - The flows between the eCCW client and the server will transit through the Internet network.
 - The internet provider is the internet provider of the user.
 - The eCCW service will be accessed from any user workstation located within the company LAN like any other Internet-based application besides the authentication that must take place using the Secure id process.

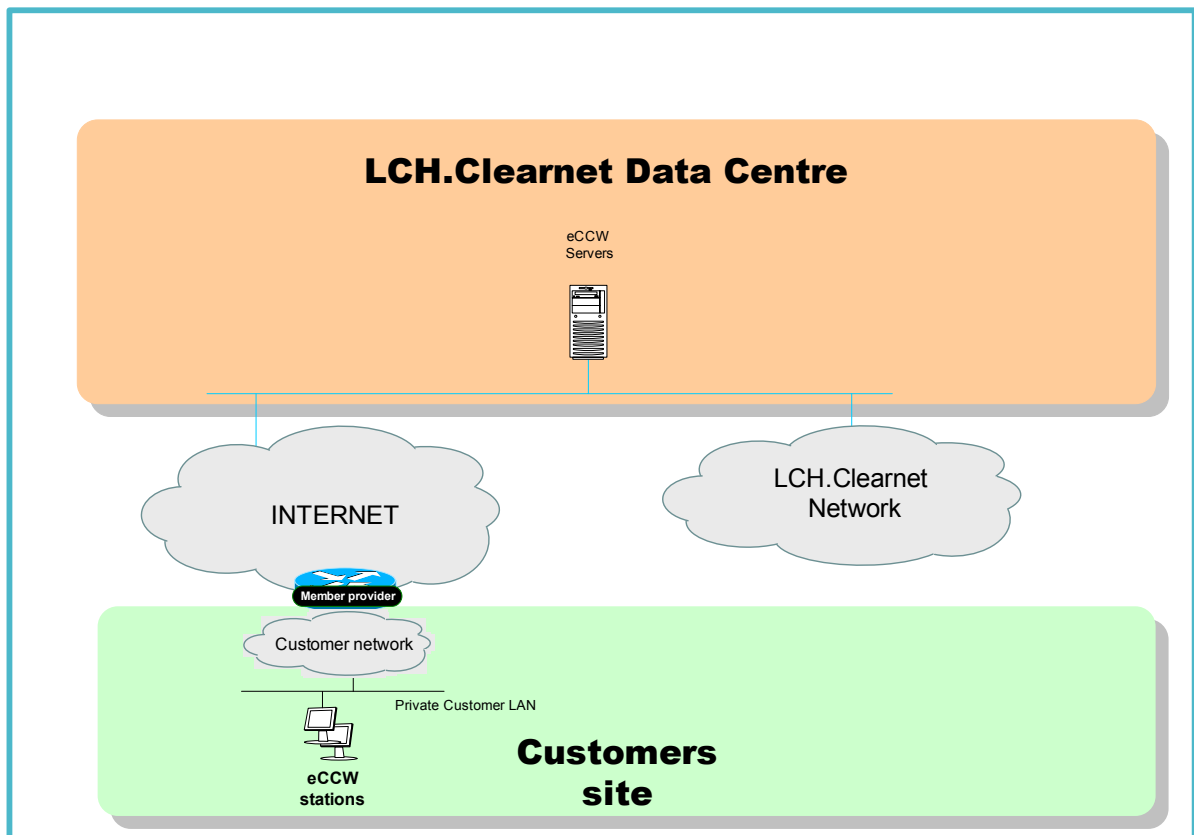


Figure 1

2.2.2 eCCW over MSA

- User Private LAN Solution Characteristics (See Figure 2 – Left side)
 - The flows between the eCCW user and the server will transit through the LCH.Cleartnet private network. (Leased lines)

- The user workstation is hosted on the user company LAN.
 - Each workstation that requires access to eCCW must encompass a eCCW source address translation under the responsibility of the user.
 - A different URL should be used to reach eCCW server through Internet or through the LCH.Clearnet network.
- **LCH.Clearnet Public LAN Solution Characteristics (See Figure 2 – right side)**
 - The flows between the eCCW user and the server will transit through the LCH.Clearnet private network. (Leased lines)
 - The user workstation is hosted on the LCH.Clearnet public LAN located at the user office.
 - The user workstation is therefore dedicated to a eCCW usage.

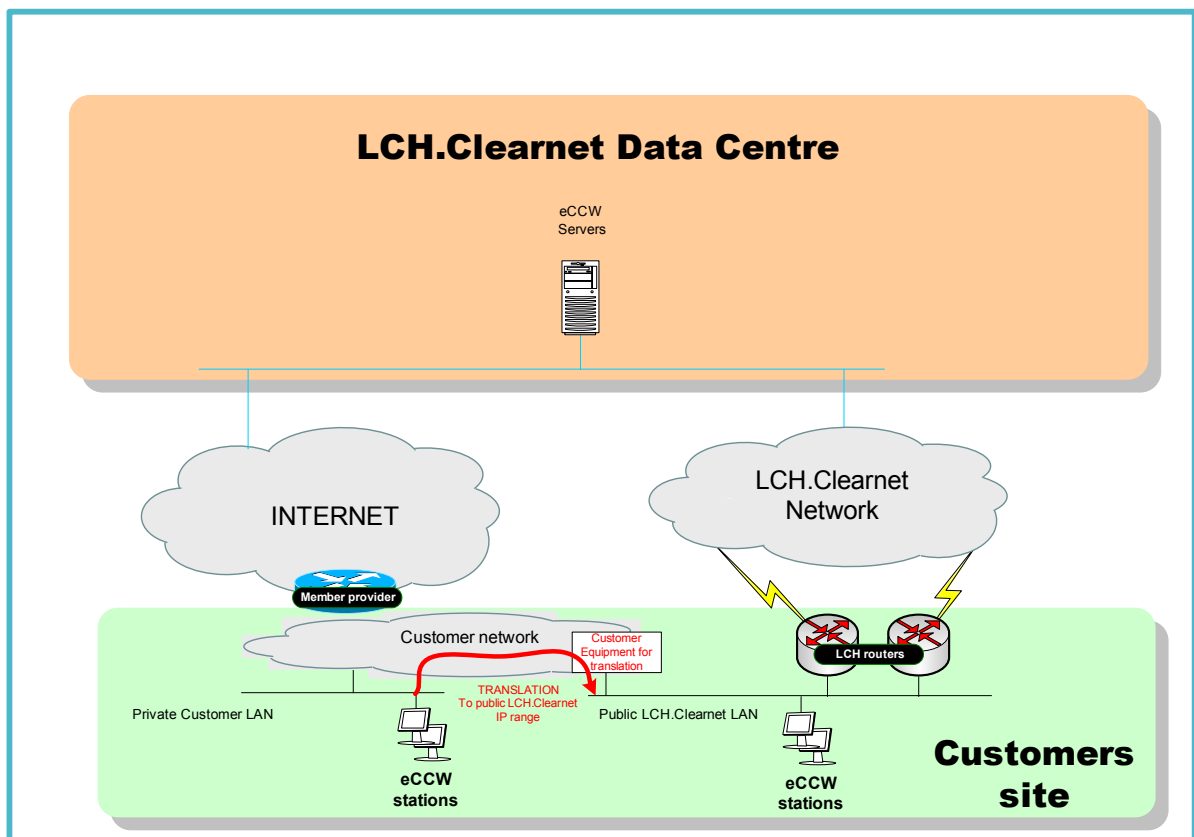


Figure 2

2.2.3 eCCW over Dedicated Access

It is important to note that the dedicated access solution runs over a 64Kbps leased line and therefore there is a limitation in using the eCCW file download function which will impact the real time application.

- **Customer Private LAN Solution Characteristics (See Figure 3 – left side)**
 - The flows between the eCCW user and the server will transit through the LCH.Clearnet private network (leased lines.)
 - The user workstation is hosted on the user company LAN..

- Each workstation that requires access to eCCW must encompass a eCCW source address translation under the responsibility of the user.
 - A different URL should be used to reach eCCW server through Internet or through the LCH.Clearnet network.
 - The dedicated Access 64 Kbps leased line is limited to three devices (eCCW or CCW).
- **LCH.Clearnet Public LAN Solution Characteristics (See Figure 3 – right side)**
 - The flows between the eCCW user and the server will transit through the LCH.Clearnet private network. (Leased lines)
 - The user workstation is hosted on the LCH.Clearnet public LAN located at the user office.
 - The user workstation is therefore dedicated to a eCCW usage.
 -
 - ECCW over dedicated access has the same constraints as running over MSA.
 - The dedicated Access 64 Kbps leased line is limited to three devices (eCCW or CCW)

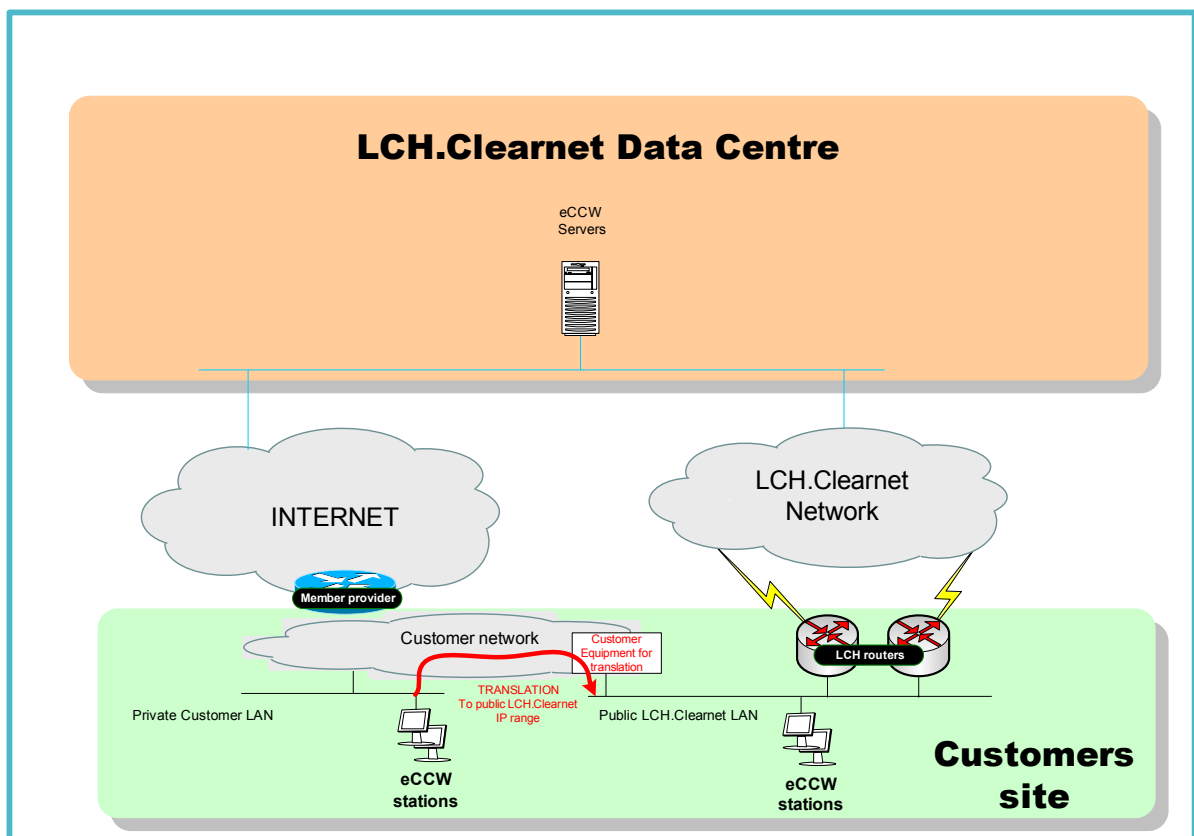


Figure 3

3 eCCW Services

3.1 Mains principles:

3.1.1 eCCW Members Security Administrators (EMSA):

- Each customer must nominate at least one eCCW Security Administrator (EMSA) who will manage user access for their organisation through local procedures which manage:
 - The orderform to eCCW
 - The whole users eCCW access cards
 - The PIN code for users
 - Change management of eCCW access cards

For more detail concerning EMSA definition, please refer to Appendix 1 of the Order Form.

3.1.2 eCCW access card authentication:

- Users will require a unique **username**
- **A user name** in an organisation is linked to one and only one token in a given environment and must be unique to the organisation in that environment (i.e. Production or user Test)
- User names will be provided by the LCH.Clearnet **on request** on the Member
- User names shall be meaningful enough to uniquely identify the user
- User names will be based on first and last name of users

For your information, please note that very short names and generic names for job roles will be prohibited.

3.1.3 eCCW package includes:

- 2 eCCW access cards (1 for production and 1 for testing)
- Optional : 1 eCCW access card to Backup

3.1.4 Profile options:

- Read & write
 - Definition: full access on consultation & command
- Read Only
 - Definition: Access only on consultation
- Access
 - Definition: specify the products and user codes that the login will be granted access to
 - Cash or/and Derivatives

4 User general Information of a eCCW access card



4.1 Mains principles :

- You are responsible for the authentication tools which have been provided to you.

- **The PIN code** is a code only known by the user. This code is unknown by the card: the latter does not have a chip enabling it to record the Pin code, like a bank card, the card only mixes the code entered by the user and the code displayed on the screen.

. Before your first connection, LCH.Clearnet will deliver initial PIN codes to the EMSA (upon your request).

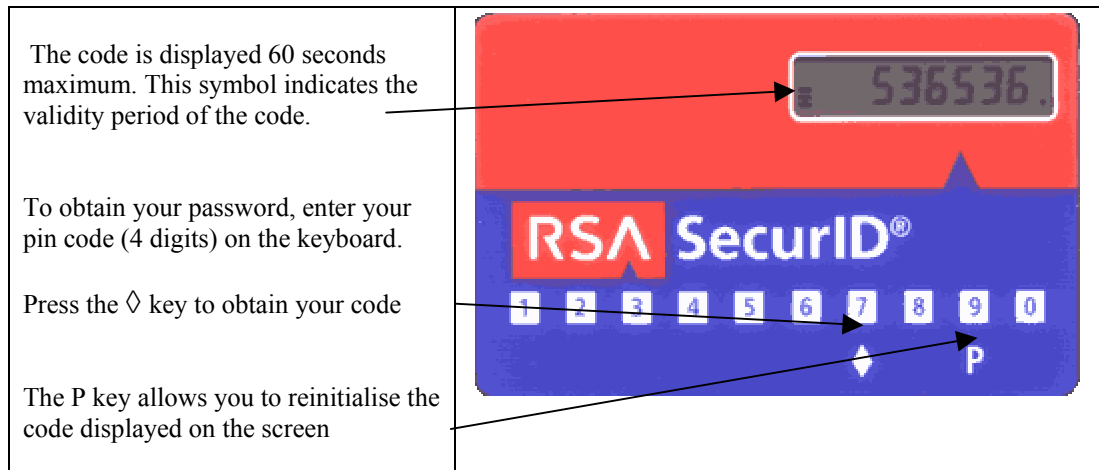
The eCCW access card displays a code which changes every 60 seconds (If you have not entered your PIN code, the displayed code does not enable you to authenticate yourselves.

- **The Passcode** is the combination of the Pin code and the code displayed by the card. The PASSCODE must be entered at the time of your connection.

Note: for confidentiality reasons, the PASSCODE is not displayed on the computer screen at the authentication time.

4.2 eCCW access card picture

The eCCW access card generates passwords which are usable only once.



•