



## ePoster 3 – Technical White Paper

Last updated 6 April 2004

This paper addresses various technical aspects related to ePoster 3. Information about how ePoster works, how to use the software, and the installation process, is available in the main ePoster help file, which can be downloaded from <http://leong.com.au/ePoster/ep3help.chm>.

If you have further technical queries, please contact the software developer, Leong Software, by emailing [info@leong.com.au](mailto:info@leong.com.au).

## Contents

1 Underlying model.....	1
2 Architecture model .....	2
2.1 LAN Configuration .....	2
2.2 http Protocol Configuration .....	2
3 ePoster and Laptops .....	2
4 Network Issues .....	3
4.1 Network Traffic.....	3
4.2 Frequency of Local Updates.....	3
4.3 Managing Wide Area Networks with Low-Speed Links.....	4
4.4 Impact on ePoster of Network Interruptions .....	4
5 Access to Channels.....	4
6 Security in ePoster .....	4
6.1 Passwords .....	4
6.2 Security of the ePoster list and poster files .....	4
6.3 Security of Alert messages.....	5
7 Setting up ePoster.....	5

### 1 Underlying model

ePoster is built on a “client-side” or “demand-side” model. End users decide which channels they want to subscribe to. When a user's screensaver is activated, ePoster then checks what channels the user has subscribed to, and displays posters from these channels.

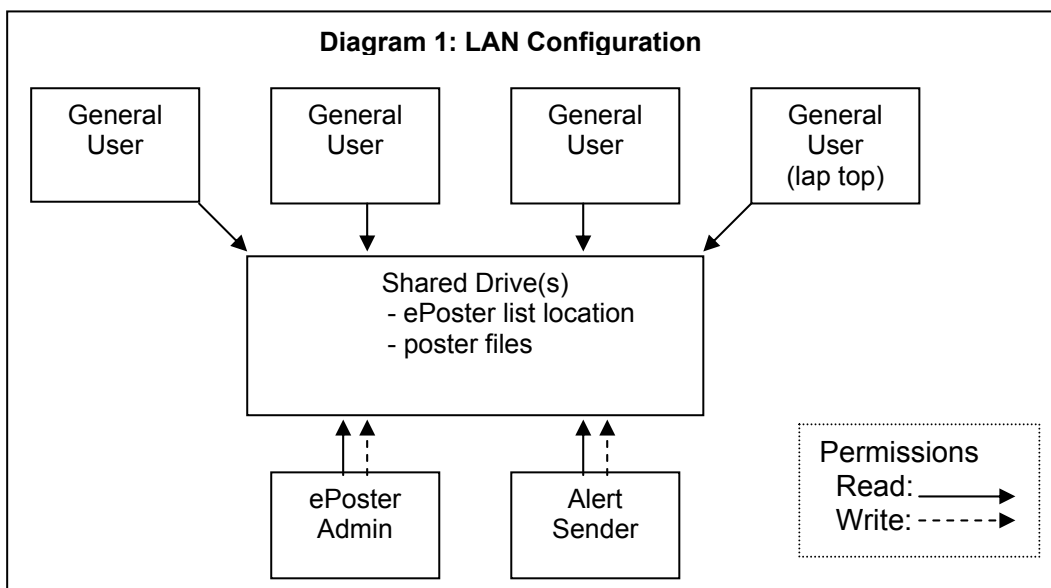
The difference can be compared to two different ways of selling newspapers. In the supply-side model, a distributor delivers the papers to each customer individually, and would need to know who wanted which newspaper. That is a lot of work, especially given they need to keep all this information up-to-date as customers come and go.

In the demand-side model which ePoster uses, the distributor just puts the newspapers in the shop, and the customers come along and decide which papers they want to buy. This lets them change their preferences at any time without creating any work for the distributor.

## 2 Architecture model

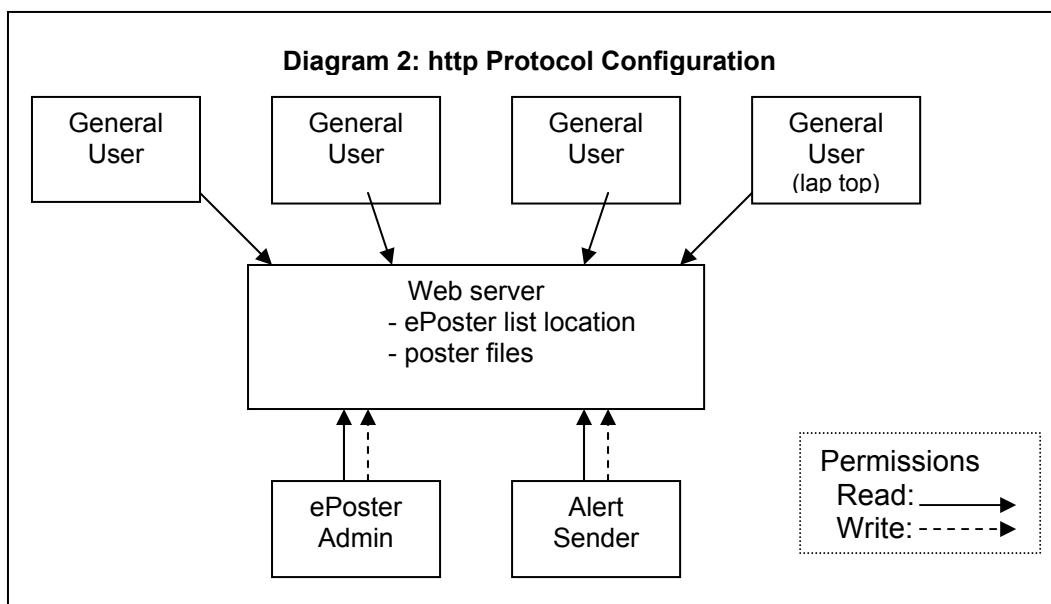
### 2.1 LAN Configuration

Diagram 1 shows the architecture model for ePoster when installed on a LAN. All users must have read permissions on the shared drive designated as the ePoster list location. ePoster Administrators and Alert Senders must also have write permissions.



### 2.2 http Protocol Configuration

Diagram 2 shows the architecture model for ePoster when configured to use http protocol. General users can be located inside or outside the firewall. ePoster Administrators and Alert Senders must be located on the same network as the web server, and have write permissions to the directory of the web server designated as the ePoster list location.



## 3 ePoster and Laptops

ePoster works seamlessly with laptop computers.

When the laptop is connected to the network, ePoster updates the ePoster list as normal, and caches all poster files under the user's profile on the laptop.

When the laptop is being used offline, ePoster will continue to display posters as normal, according to the settings from the last time the laptop was online. As soon as the laptop is reconnected to the network, ePoster will automatically update and download files as needed.

## **4 Network Issues**

### **4.1 Network Traffic**

IT areas are often concerned whether ePoster will significantly add to network traffic. The short answer is that there will be no noticeable impact. The following explains why.

ePoster minimises its impact on the network by keeping a local copy of all poster files, and of the master ePoster list, under the user's profile. Whenever the screensaver or browser mode is activated on a user's computer, ePoster uses these local copies to display posters. The frequency at which ePoster checks for updates of these files can be modified by the ePoster Administrator – see section 4.2 below.

A separate process checks for Alert messages. This occurs every 1-2 minutes, to ensure that messages reach users as quickly as possible. The process compares the dates of two files, and is tiny in network terms.

When the network is set up to store user profiles on local computers, there is therefore no impact at all on the network when a user is viewing posters in either screensaver or browser mode. If the network environment uses roaming profiles – ie the profiles are stored on the server – then there would be slight increased network traffic when users log on and off.

A web page is about the same size as an email with the same content and formatting. Replacing emails with web format posters containing the same information will therefore make no difference to network load. It may even reduce network load, if "all staff" emails are turned into channel-specific posters, which only a sub-section of the user base will choose to include in their channel list.

Ultimately, the overall network impact of ePoster is determined by the file size of the posters which the organisation uses. The organisation can therefore control this by controlling what types of posters it uses. The following points will be useful:

- Simple posters such as text-only web pages have smaller files than posters with pictures or animation.
- Flash files are usually relatively small.
- PowerPoint, Word, picture and movie files are usually relatively large.

### **4.2 Frequency of Local Updates**

To keep its data current, each ePoster computer checks the currency of its local master list and poster files at regular intervals. Even if all users log on at exactly the same moment, ePoster uses a randomisation process to spread out the timing of these checks.

The update process compares the modified date of the local file with the modified date of the master file – a very small transaction, about as noticeable on the network as an ant on a highway.

- If the two dates are the same, nothing further occurs.
- If the dates of the master lists are different (ie the master list has been updated), ePoster will make a new local copy of the master list, and of any new posters, under the user's profile. The list file is very small – for example, a typical list file with 100 posters is about 14KB.
- If the dates of a poster file are different (eg a PowerPoint presentation has been updated), the local computer will make a new copy of the poster file. This would have the same network impact as downloading the same file from the intranet.
- Note: For web format posters, the files are kept up-to-date using Internet Explorer's standard processes.

This frequency of local updates can be set at one of four options – every 5 minutes, every hours, every four hours, and on start-up only. A higher frequency is more suitable when posters are added or updated regularly, or it is important that new posters reach the users quickly. A lower frequency is more suitable when posters are not added or updated often, and/or the priority is to reduce network load. Note that a lower frequency means that updated information will take longer to reach the end users.

### 4.3 Managing Wide Area Networks with Low-Speed Links

If an organisation has a Wide Area Network with some locations serviced by low-speed links, network traffic can be minimised by the strategic use of channels. Specific channels should be set up for the low-speed locations, and only posters with a small file size allocated to these channels (see section 4.1 above). Users in these low-speed locations should be advised to only subscribe to these channels.

The ePoster Administrator should also set the frequency for local updates to a lower setting, such as "on start-up only".

### 4.4 Impact on ePoster of Network Interruptions

As ePoster keeps local copies of all data files, there is very little impact from a network interruption. The screensaver and browser modes on local computers will continue to display all posters which were available before the network interruption. When network services are resumed, each local computer will automatically check for updated files as usual within 1-2 minutes, as explained above in section 4.1.

## 5 Access to Channels

Access to channels is controlled by the ePoster Administrator choosing whether to allocate a password to a channel. This is done through the Channels screen of ePoster Admin.

A channel with no password can be selected by all users. They do this through the Channels button in their browser mode.

To add password-protected channels to their channel list, each user must have the channel's password, which is set by the Administrator. These passwords are distributed to users through non-ePoster mechanisms. (See "security" below for more information).

## 6 Security in ePoster

### 6.1 Passwords

Passwords apply only to channels, and are created by the ePoster Administrator. The only time a user enters a password is when they are trying to add a password-protected channel to their channel list. They do this using the password which is supplied to them (independently of ePoster) by the ePoster Administrator or another person designated by the organisation.

For example, an organisation might set up a password-protected channel for senior managers across the organisation. The password will be created by the ePoster Administrator when creating the channel in ePoster Admin. He/she might then provide the password to the executive assistant in each division, who would then be responsible for giving the password to all senior managers in that division (and to new senior managers as they arrive). Senior managers would only start viewing posters from that channel once they had added it to their channel list.

If there is a need to change the password, this would be done by the ePoster Administrator. All senior managers would immediately lose access to the channel. The new password would need to be distributed to the managers, and they would need to add the channel to their lists again.

When ePoster queries a password across the network (when a user adds a password-protected channel), it is always in encrypted form. Each licensed version of ePoster uses a different encryption key.

Note: Each organisation should make its own determination of whether it is appropriate to use ePoster's password-protected channels for communicating sensitive information. For example, if offices are open-plan or visitors to an office have easy view of the computer screen, it would not be appropriate to use ePoster to share sensitive information.

### 6.2 Security of the ePoster list and poster files

ePoster uses three list files to contain its data. These are located in the "ePoster list location" specified by the ePoster Administrator as part of the set-up process (see Phase II of the Setting Up ePoster section in the ePoster Admin help file).

The organisation sets appropriate permissions for this directory. The ePoster Administrators and Alert Senders need write permissions, but all general users should have read-only permissions. This prevents general users from touching the ePoster list files. Only the Administrators have the software (ie ePoster Admin) to actually make any changes to the list.

All posters are "cached" under the user's profile. Data is not accessible by any other user on the network (except for system administrators).

In highly sensitive situations, the organisation should use its normal network file permissions to control access to high-security poster files. If an unauthorised user somehow managed to add a password-protected channel to their list, the network file permission structure would still deny any unauthorised access to the files, and ePoster would not be able to display the posters.

### 6.3 Security of Alert messages

A number of barriers prevent an unauthorised user from sending an Alert message:

- General Users do not have the Alert software installed on their machine
- if ePoster is set up as recommended in section 2 above, General Users do not have write permissions on the ePoster List Location, and therefore cannot create Alert messages
- each Alert Sender must set up their own Alert password, which is kept in encrypted format under the user's profile. There is no limit to the character length of the password.
- at the time of sending an Alert message, the user must re-enter their Alert password. This prevents an unauthorised user sending a message from an Alert Sender's computer.

All Alert messages identify who authorised the message (as entered by the Alert Sender), and who sent it (generated automatically by ePoster from the user name and the computer name). Having these two levels of identification means that:

- people whose name might not be recognised widely can send messages on behalf of higher profile staff – eg the secretary to the Head of Corporate Services
- you always know who actually sent the message, and which computer they sent it from.

## 7 Setting up ePoster

Setting up ePoster is a straightforward process. It comprises four phases:

- planning
- setting up the ePoster Administrator
- preparing for the rollout
- rolling out the software

Detailed information on each phase is included in the ePoster Admin help file, which is provided with the trial copy of ePoster.

Depending on the number of computers involved, an organisation may choose to install ePoster in one of several ways. The following table provides a guide.

Situation	Possible installation approaches
Large number of computers	Network rollout
Medium number of computers	Network rollout Email distribution
Small number of computers	One-by-one Email distribution

In organisations which are large, have multiple sites or complex network infrastructures, the IT area may choose to roll out the software in phases, rather than across the entire organisation at once. Of course, in this situation ePoster should not be used as the only way to communicate important information until it has been rolled out to all users.

Detailed information on installation approaches is also included in the ePoster Admin help file.