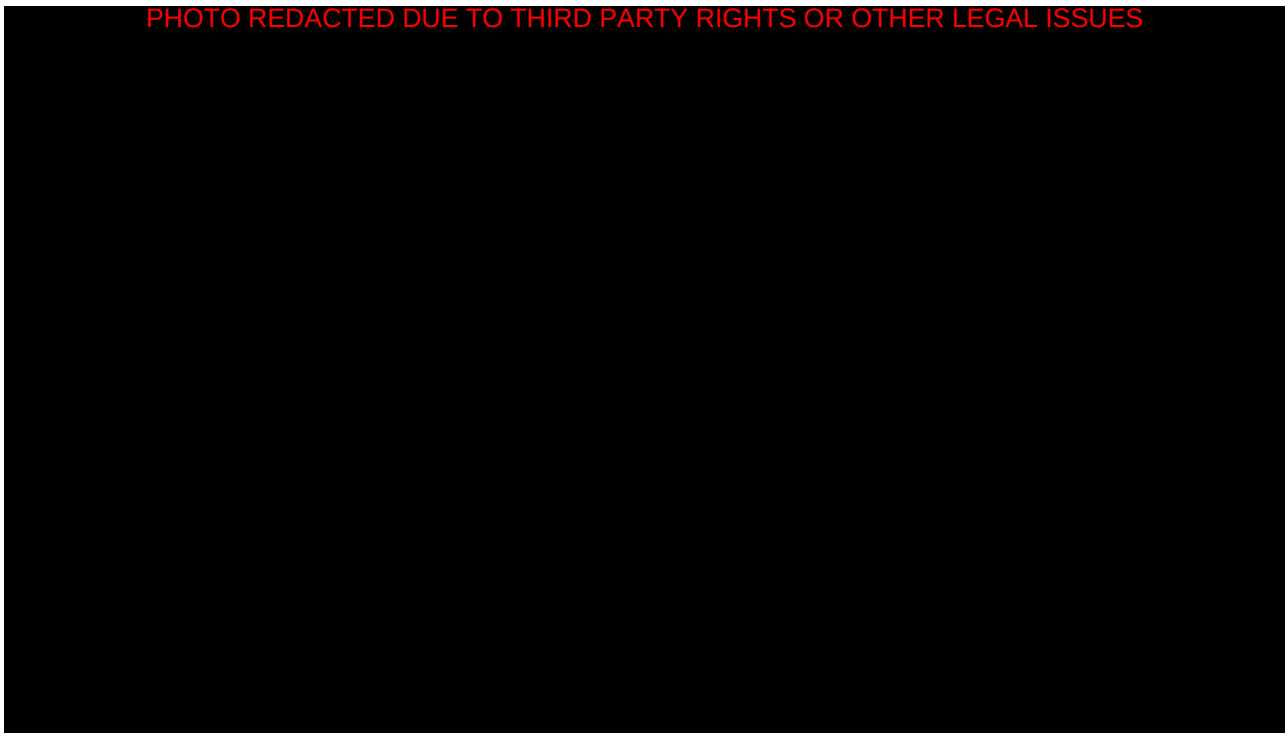
E-enablement of the Common Assessment Framework

eCAF Security Architecture

Version 1.0



Every Child Matters
Change For Children

Document Control

Revision History

Issue date	Version	Summary of Changes
08/06/2006	1.0	Initial publication

Purpose of this Document

This document is the Security View for the e-enablement of the Common Assessment Form (eCAF). Its purpose is to communicate the security requirements applicable to eCAF implementations.

Contents

Abbreviations

Term	Definition
CAF	Common Assessment Framework
eCAF	Electronic Common Assessment Framework
DfES	Department for Education & Skills
DCA	Department for Constitutional Affairs
DH	Department of Health
ECM	Every Child Matters
IWP	Integrated Working Project
DPA	Data Protection Act
FIA	Freedom of Information Act
ACL	Access Control List
AAD	Additional Access Decision

1. eCAF Documentation Reader's Guide

A number of documents define the requirements of the e-enabled Common Assessment Framework System (eCAF). The diagram below gives an overview of these documents and their relationship to each other. Notes below the diagram describe the purpose of each document.

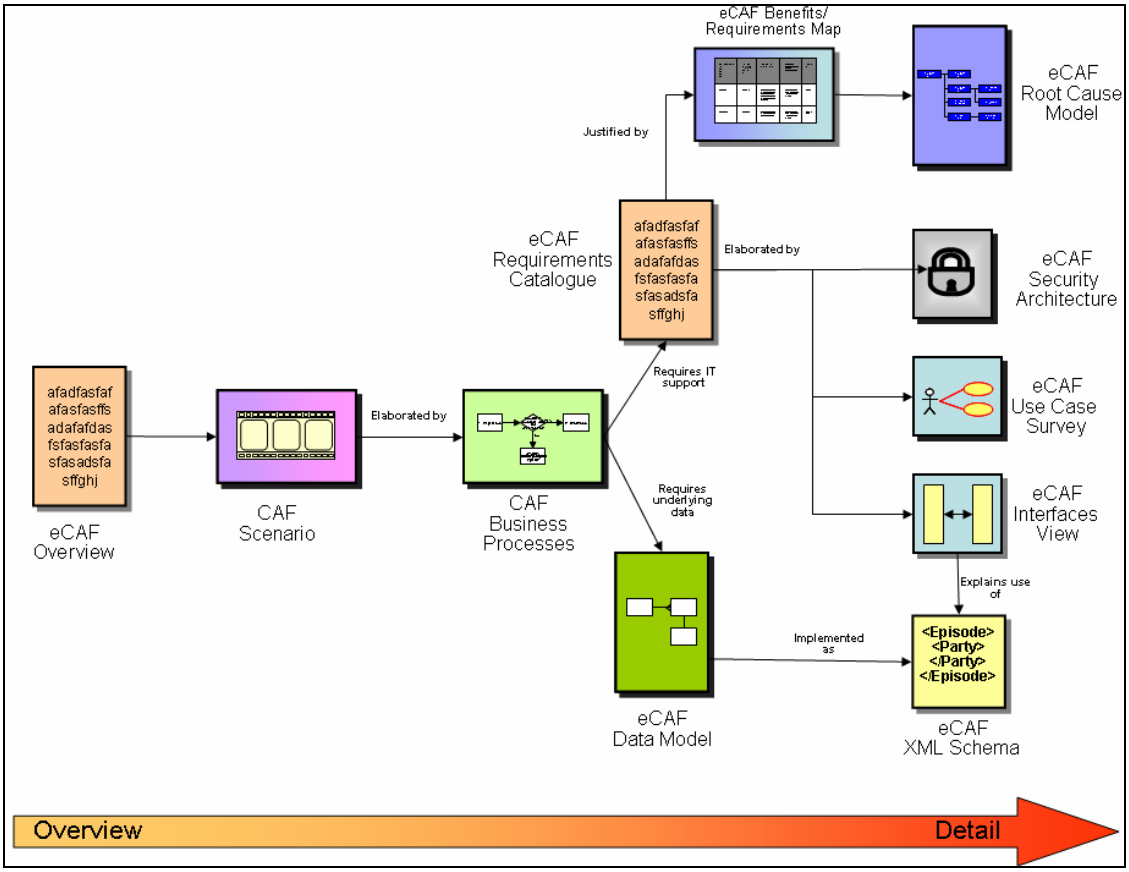


Figure 1 – eCAF Document Route Map

The eCAF document set comprises:

- **eCAF Overview** – Essential starting point and executive summary. Introduces the other documents in the set.
- **The CAF Scenario** – This document walks through a "story", showing an example of how the CAF Business Processes might work in practice. Useful for all readers, to gain a basic familiarity with CAF process.
- **The CAF Business Processes** – This document describes the people and business activities that are required to complete a Common Assessment and the subsequent actions arising out of that Assessment. It also indicates where IT support from an eCAF system will assist these activities.

- **The Requirements Catalogue** – This document defines what system support is required by practitioners using the Common Assessment Framework (CAF). It contains categorised listings of functional and non-functional requirements.
- **The Security Architecture** – This document defines in more detail the security requirements for an eCAF system. This is a critical aspect, and thus worthy of specific consideration.
- **The Use Case Survey** – This document presents the requirements as Unified Modelling Language (UML) Use Case diagrams. This may be useful for more technical readers, for example to inform the Inception and Elaboration stages of a Rational Unified Process (RUP) development project.
- **The Interfaces View** – This document provides more information about the interfacing requirements for an eCAF system. Interfacing is important but potentially complex, so this document provides additional guidance.
- **The Data Model** – This document contains a high-level diagram of the information that will be required in the context of CAF. It provides a more detailed view of information requirements in the form of an Entity Relationship Diagram that defines the essential eCAF data items and their relationships. It also includes a set of Data Classifications which summarise the types of data used in CAF, such as Name and Contact Details. It provides standard names and definitions that will be used by an eCAF system.
- **The XML Schema** – This is a technical schema specification (plus example xml file), providing a standard representation of the Data Model as an XML (GovTalk) message. XML is a widely accepted data format used for information exchange between systems.
- **The Root Cause Model** – This document describes the root causes of the main issues which prevent the delivery of the targeted outcomes of the 'Every Child Matters: Change for Children' Programme (relevant to initial assessments). It states both the business challenges faced (the issues and their root causes) and the business need to be addressed.
- **The Benefits/Requirements Map –** This document provides the linkage between the root causes eCAF looks to address and the solution components (requirements) designed to address them.

2. Introduction

eCAF is a framework for assessing children's needs and for coordinating multi-agency responses to them. An eCAF implementation will record details of episodes in a child's life, which will be accessible by a number of interested agencies such as schools, health professionals and the Police.

eCAF information is sensitive and must be protected properly from unauthorised access. This document describes what protection is required and also gives guidance on achieving a usable and interoperable implementation.

This document only covers the application-level protection of personal data. It does not address the general infrastructure security measures, such as firewalls and virus protection, that any responsible IT-aware organisation should already have.

If eCAF implementation is delegated to local authorities then the eCAF architecture (including this security architecture) will not be mandatory, and will be guidance only. Local authorities that choose not to conform to it should, however, take advice as to how they will meet their legal obligations in the information security area.

Note that this document focuses on the "what", in terms of security requirements for an eCAF system. It leaves open a number of options for the "how", in terms of the security infrastructure to achieve these requirements.

Other Every Child Matters projects (such as the IS Index) are also intending to publish security requirements and guidance in the near future. This should be reviewed, when available, to ensure a compatible approach to any infrastructure solution.

2.1 Audience

This document is intended for security architects and analysts who are working on an eCAF implementation. It may also be of interest to business and IT managers, data protection officers, and others responsible for data and system security.

It gives guidance about:

- The minimum security level that eCAF implementations should achieve, that is, the security countermeasures that should be employed.
- How to address some of the common usability and integration issues that can arise with secure systems.

2.2 Structure

Chapter 3 contains general background information that is of interest to security practitioners. Much of this information is available in other documents.

Chapter 4 contains the security background facts that drive the security requirements. This includes information about the legislation and policy that should be followed, the assets to be protected, and the users it should be protected from.

Chapter 5 then describes the security services that should be provided and gives detailed requirements for each.

Chapter 6 gives guidance on achieving interoperability and usability for (and between) eCAF implementations.

3. General Background

3.1 Organisations Involved

The DfES is a UK central government department. It sets targets and policy for UK schools and monitors conformance to these.

The DfES has initiated the development of CAF and eCAF.

eCAF may be implemented centrally or, more likely, individually by each local authority in England. Any body that implements eCAF will be responsible for operating the implementation.

eCAF users will come from any of the organisations involved in child care and protection, such as:

- Local authorities.
- The Police.
- Healthcare professionals (GPs, midwives, other professionals).
- Schools and other organisations involved in education.
- Voluntary organisations (such as Barnados).

Where eCAF implementation is delegated, because each type of organisation will have different geographical boundaries, there will be a need either for eCAF implementations to synchronise data to give their users a complete view, or for users to access several different eCAF implementations. Also, eCAF implementations will need to share data when data subjects move around the country.

The total population of eCAF users is expected to be around 200,000.

3.2 The eCAF Process

eCAF provides a generic process for addressing needs. This process is in three stages:

- Preparation, to decide whether a full assessment should be performed and to determine the agencies involved.
- Discussion, perform an assessment of the child's needs. This can be done either by a single agency or by multiple agencies. A set of action points will be agreed for the agencies to perform.
- Delivery, complete the agreed action points.

Assessments can be performed for children aged up to 18, for people with special needs up to 25, and for unborn children.

4. Security Drivers

4.1 Applicable Regulations

The principal legislation that eCAF is concerned with is as follows:

- The Data Protection Act (DPA). Personally identifiable data concerning children comes within the scope of this act. The act requires data holders to be registered with the Information Commissioner, and to apply eight data protection principles. These include -
    - Data must be protected in a way that reflects the harm that its compromise could cause.
    - Data must be collected with the subject's consent and must be distributed and processed with the subject's consent.
    - Data subjects have the right to view what is stored relating to them.
- The Freedom of Information Act (FIA). This allows citizens to make information access requests on government data. Part of the FIA requirements would be met by conforming to the DPA, the remainder should be met using an organisation's existing FIA measures. Therefore the FIA will not be considered further here.

In order to encourage the growth of eCommerce, the eEnvoy has developed an eGovernment Security Framework that specifies security requirements for g2c e-commerce. This specifies 4 levels of requirement for the following security services:

- Confidentiality
- Registration
- Authentication.
- Non-repudiation.

Each eGovernment security service must protect its services at the right level. The meaning of the levels is as follows:

- Level 0 is for public data and requires no special security (other than availability)
- Level 1 is for data that is not public but would cause little damage if compromised, for instance name and address.
- Level 2 is for data which is private and must only be given to known individuals. For instance, tax returns.
- Level 3 is for data which is sensitive and must be protected against accidental or casual compromise. This is equivalent to the RESTRICTED protective marking. For instance, medical records.

4.2 Actor Types

eCAF must cater for the following types of human user:

- Practitioner users. These access an eCAF implementation in a professional capacity to carry out or advise on an agency's response to a child's needs.

There are two types of practitioner user, depending upon the way they are managed:

- Personal users. These are people who have legitimate individual access to an eCAF implementation. However, they are not given access by an employer.
- Sponsored users. These users are registered and managed by an authorized body (such as a Police force or a local authority) which sponsors their access.

An episode team will be made up from practitioner users. The eCAF Requirements Catalog partitions practitioner users into CA Episode Administrators, Contributing Practitioners, Viewing Practitioners and Supervisors. These are different roles that a practitioner can have with respect to a particular episode.

- System administrators. These administer an eCAF application or its hosting infrastructure using operating system and database facilities. They will administer the eCAF users. Each application or operating system is likely to be managed by a different class of administrator, each with its own permission set. System administrators can be practitioners as well but, given the different skill sets involved, this situation will not be common in practice.
- Developers. These test and develop eCAF applications and implementations.
- Citizens. These are children and those associated with them.
  - Children. These are the children whose details are recorded in an eCAF implementation.
  - Carers. These are people (normally parents) with a legal responsibility for a child.
  - Others (could include family members).

  Note that direct access to eCAF by citizens is considered out of scope as a business requirement. This does not mean that such access is forbidden, but it does mean that the security measures required are not defined in this document.
- Data subject. A data subject is someone who has personal data recorded within eCAF (which can include practitioners and citizens). Both practitioners and citizens can be data subjects.
- Consentor. This is someone who consents for a data subject's data to be stored and processed within eCAF. In most cases this will be the data subject himself but where the subject is not legally competent, it can be the carer or some other person.

An eCAF implementation is likely to interoperate with the following types of external system:

- Other eCAF systems.
- Other applications, such as case management tools, operated by authorized bodies as described in Section 3.1.
- The Index System, an index of children being developed independently under the auspices of the DFES. The Index System will have contact details each child and a marker indicating whether the child is handled in a CAF system.

4.3 Security Domains

We need to consider a range of areas from which an eCAF implementation can be accessed:

- Authorised body premises and networks.
- Mobile access, Internet access and access from insecure areas. Additional countermeasures will be required for access from or across such as domain.

4.4 Data Classifications

It is critical that a proper balance is found between the need to protect eCAF data, and the cost/inconvenience of doing so. The first step to achieving this balance is to understand the importance of the data being protected.

In this document we will follow the 'e-Government Strategy Framework Policy and Guidelines' standards issued by the Cabinet Office. These standards describe how to categorize the requirements for each of the 4 security objectives (confidentiality, integrity, availability and non-repudiation), see 4.1. They do so by measuring the impact of a compromise to each objective. This leads to 4 separate 'values' for each piece of data. Each 'value' then guides the implementation of a set of security services.

4.4.1 Confidentiality

Confidentiality is a property of data, that it has not been revealed to the wrong people. The following table indicates the confidentiality levels for the broad categories of eCAF data.

Data Type	Confidentiality Level
Episode and episode item data	Level 3
Episode role data	Level 3
Contact details for children, carers and practitioners.	By default, these details will be at level 2. However, some (for instance, children of VIPs) will be more sensitive (level 3). A facility is required for marking such records.
Organisation details	Level 0
Relationships between parties	By default, these details will be at level 2. However, some will be sensitive, for instance, the identity of a child's father may be sensitive in some cases, and links to particular types of practitioner will allow inferences to be made about episodes. A facility is required to mark certain links as sensitive.
Access Control Lists (ACLs) and Additional Access Decisions (AADs)	Level 3

Audit logs	Level 3

What this table states is that episode data is about as sensitive as medical records, that is, that a high level of protection is required for them. Role relationships are equally sensitive because they could allow inferences to be made about a child's problems. Most contact details, however, are less sensitive (while still not being public).

4.4.2 Integrity

Integrity is a property of data, that it is correct and has not been tampered with. All the eCAF data is at an integrity level of 3.

4.4.3 Availability

Availability is a property of data, that is available when needed and has not been deleted. Each eCAF implementer must carefully consider what level of availability protection is required for its data, for instance, what recovery time would be acceptable in the case of a disaster.

4.4.4 Non-repudiation

Non-repudiation is a property of data, that it is not merely correct, but can be demonstrated to be correct to a third party, such as a court of law in a criminal prosecution.

Non-repudiation is not a requirement for eCAF because eCAF will not be the only source of information about how a child's needs were analysed or addressed – for instance, information can be gleaned from other applications, formal communications, and personal recollections.

eCAF implementers can, of course, choose to implement non-repudiation services if they wish, though the costs can be considerable.

4.5 Privacy and Consent

The most important security driver for eCAF is the Data Protection Act which requires data subjects to give consent before their personal data is stored and processed in an information system (see 4.1).

The detailed process for child data is specified in the eCAF Business Processes specification and a summary is given below.

Every episode is associated with an assessment describing the child's needs and the actions to be taken to meet those needs. The assessment includes a section to record consent by or on behalf of a data subject.

Consent could be a blanket consent, a collection of tick boxes indicating the agencies that may receive the data, or a natural language narrative describing the data subject's detailed requirements. These can be arbitrarily complex. Consent is recorded by having a paper printout of the assessment form signed by, or on behalf of, the data subject.

In most cases the child (or his carer) will be given a copy of the assessment form. This can be refused if the child could be harmed as a result.

Each episode may have a number of users with access rights assigned:

- Full Control – able to update the Episode data and also to manage access rights for other users. This is intended primarily for the Episode Coordinator - the human user who is ultimately responsible for the episode. However the Episode Owner may also choose to grant this access right to other practitioners, so that they can deputise as “Episode Administrators”.
- Update – able to update the Episode data, but NOT to manage access rights for other users. This access right may be assigned by the Episode Owner to allow other practitioners working closely with the child to add information to the Episode themselves
- Read Only – the default for practitioners other than the Episode Coordinator. Able to view the Episode data but not to make changes.

Every episode is associated with an Access Control List (ACL), and with any number of Additional Access Decisions (AAD). An episode’s ACL is an interpretation of the natural language consent agreed with the data subject, and gives access to members of the episode team. An AAD covers any additional access requirement, such as one-time access by someone not in the episode team, or access granted without the data subject’s consent. In the latter case, an AAD must be justified by one of the waivers specified within the Data Protection Act, and the justification will be recorded along with the AAD. The use of AADs should be exceptional. An AAD should be time-limited; ACL entries can be time limited.

ACL entries and AADs are controlled by episode administrators.

Every episode is associated with an access log that records read and write access to the assessment and changes to the ACL and AADs.

Note that eCAF will contain some personal data (mainly contact details) about practitioners. Since practitioners need to use eCAF in order to perform their jobs, they do not need to explicitly give consent for their data to be stored. (Note: a legal opinion may be required to confirm this).

4.6 Security Services

eCAF implementations should protect data by implementing the following security services:

- Registration (the process of adding users to the system).
- Authentication (the process of checking user identities).
- Access control (restricting access to data).
- Audit (recording user activity).
- Encryption (scrambling data to make it unusable).

Chapter 5 specifies full requirements for each service. It also briefly discusses security infrastructure requirements.

5. Security Services

Here we specify requirements for each of the services listed in Section 4.6.

5.1 Registration

Registration is the process of creating eCAF users, administering them, and removing them.

It is very important that individuals' identities are checked before they are given access to eCAF. We will use the eGovernment Security Framework which defines 4 registration levels, 0-3, with level 0 involving no identity checking and level 3 involving the most rigorous checks. Refer to 'HMG's Minimum Requirements for the Verification of the Identity of Individuals' for details of each level. A similar set of criteria has been defined for checking the identity of an organisation.

The following checks must be performed for eCAF users:

- Practitioner users must have their identities checked at level 3. They must also produce documentary evidence for their practitioner status, for instance, academic qualifications or an employment contract. They must also be subjected to a Criminal Background Review and must be checked against the sex offenders register.
- System administrators must have their identities checked at level 3. They must also be subjected to a Criminal Background Review and must be checked against the sex offenders register.
- Developers do not require identity checks.
- Data subjects must have their identities checked at level 3 before being given electronic access to an episode. Carers must have their identities checked at level 3, and must show documentary evidence of their relationship to a child, before being given electronic access to a child's episode.

Any organisation that wishes to sponsor staff must have its identity checked at level 3.

The registration process will:

- Verify the user's identity and status.
- Obtain the user's agreement to abide by the system's conditions of use.
- Ensure that the user has sufficient training and knowledge to use the system correctly.
- Provide the user with a credential (such as a token or a password) that can be used to logon to the system.
- Give the user the necessary privileges to use the system.

A process will be required to renew or replace a lost credential. A user's identity must be checked as part of the process. Where the old credential is still working, this can be used; if it is lost or malfunctioning, it may be necessary to repeat the registration-time identity check.

Practitioner users and system administrators must have their access revoked when they terminate their employment or stop working in a practitioner or system administrator capacity. This is normally done by removing their access permissions, revoking their credentials and disabling their userID. Ideally this should be done automatically as part of the leaving process. Where automation is not possible, a manual de-registration process must be defined, supplemented by a periodic check, performed every 6 months, whereby managers reassess their users' access requirements and rescind any access which is no longer required.

5.2 Authentication

The eGovernment Security Framework defines 4 levels of authentication:

- Level 0 – no authentication.
- Level 1 – basic strength authentication. A password is required which shall be stored and transmitted encrypted. A minimum password length of 8 characters is required. Users may select any password subject to the length requirement. Users may change their password. Passwords must be changed every 90 days.
- Level 2 – certificate or (deprecated) password.
- Level 3 – high strength authentication using a hardware token.

Where data is being accessed over the Internet, the authentication level required is the same as the confidentiality level for the data. So, level 3 authentication is required in order to access an episode over the Internet.

Where level 3 data is being accessed internally, a token is still preferred, but it is not mandated, and a password (level 2 authentication) is acceptable. For this to apply:

- The whole of the network between the system and the user must be trusted, that is, it must be physically secure and it must be managed by the eCAF operator or a trusted organisation.
- The user must be working within the eCAF operator's premises or those of a trusted organisation. In particular, the user must not be mobile or working from home.
- Where an eCAF system permits both internal and Internet access, it must be able to clearly distinguish the two though network architecture or firewall rules.

5.3 Access control

Unauthenticated users must not be given access to an eCAF implementation.

The access rules for authenticated users are as follows:

Developers

- Developers must not be given access to a live eCAF service.

Practitioners

- Practitioners may read or append episodes where consent has been given or where a waiver to the Data Protection Act applies (see 4.5). Access to an episode gives read access to its access log, ACL and AADs.

- Practitioners may access any non-sensitive (level 2) relationship. For sensitive (level 3) relationships, practitioners may read or change relationships that relate to an episode they have access to.
- Practitioners may read contact details for any non-sensitive (level 2) party. For sensitive (level 3) parties, practitioners may read or change contact details for parties that relate to an episode they have access to.
- A privileged subset of practitioners may view access logs for any episode.
- A privileged subset of practitioners may create AADs, or nominate additional episode administrators, for any episode.

System Administrators

- A privileged subset of system administrators may change reference data.
- A privileged subset of system administrators may create, administer and delete practitioner users and system administrators.
- It is forbidden to change or delete access logs, but a privileged subset of system administrators may archive them.
- A privileged subset of system administrators may archive episodes.
- System administrators are not permitted access to any level 3 data. Note that it is often difficult to enforce this rule in practice, so it may be necessary to develop contractual usage conditions for these users.

Citizens

- Citizens may usually access their own contact details, episodes and relationships electronically or in paper form.
- Carers may usually access their child's contact details, episodes and relationships electronically or in paper form.
- Exceptionally, the episode coordinator may decide that these accesses are not in the child's interest, in which case he will give less or no access.

All users

- Reference data is public and may be read by any user.
- Organisation data is public and may be read by any user.

Episode items are never modified. However a user may append new episode items. Each episode item is associated with the user who added it and with a timestamp for when the addition was made. It is important that the timestamp and userID are protected from tampering.

When eCAF exchanges data with another program (including another eCAF):

- If the program is untrusted it will act with the privileges of the invoking user or the group of users on whose behalf it operates.
- If the program is trusted it will act with the privileges of an application-specific userID. A 'trusted' program is one which obeys the rules defined within this security architecture.

Once data has been transferred to a foreign trusted program, the episode administrators within that program are responsible for ensuring that the ACL within that program accurately reflects the existing consent statement and that AADs are granted under proper waivers. Note that as soon as an episode is stored in more than one program, there is a danger that the versions of the episode will start to diverge. This can be addressed by synchronizing the versions, or by designating one as the master and making the other read-only and marking it as historical.

5.4 Audit

Each system user must be associated with enough information to allow him to be contacted.

The following events shall be audited:

- All changes to data and relationships.
- Read access to level 3 data.
- Import and export events.
- Archive events.

The following information must be recorded with each audit record:

- The identity of the user involved (this must identify a human user; a group or organisation is not acceptable).
- The time.
- Sufficient data about the record changed or examined to uniquely identify the episode concerned.
- Where access is obtained under a waiver (i.e. an AAD), the reason for the waiver.

Note that, where a change is made, there is no requirement to audit a complete description of the change (i.e. what the record looked like before and after the change).

Note that where an episode is accessed in more than one program, each program must follow the audit rules. In addition, the audit logs generated by all the programs must be consolidated together in one place so they can be examined in a unified way.

5.5 Encryption

Data at confidentiality level 2 or above must be encrypted when in transit over the Internet or any insecure network. Data at confidentiality level 3 must be encrypted when in transit outside a secure data centre.

Note that encryption is not required for confidentiality level 3 (or lower) data in transit over a network which has been formally accredited to RESTRICTED, such as the GSI.

5.6 Security Infrastructure

An eCAF implementation must be housed within a secure infrastructure. We would expect organisations implementing eCAF to already have such an infrastructure so will not provide detailed guidance.

An eCAF service infrastructure should conform to ISO17799, the eGovernment Security Framework and the Manual of Protective Security. eCAF services should aim at meeting the security requirements for connection to the GSI or GSX, regardless of whether or not they do in fact connect.

5.7 Summary

Figure 5-1 below summarizes the required security services graphically.

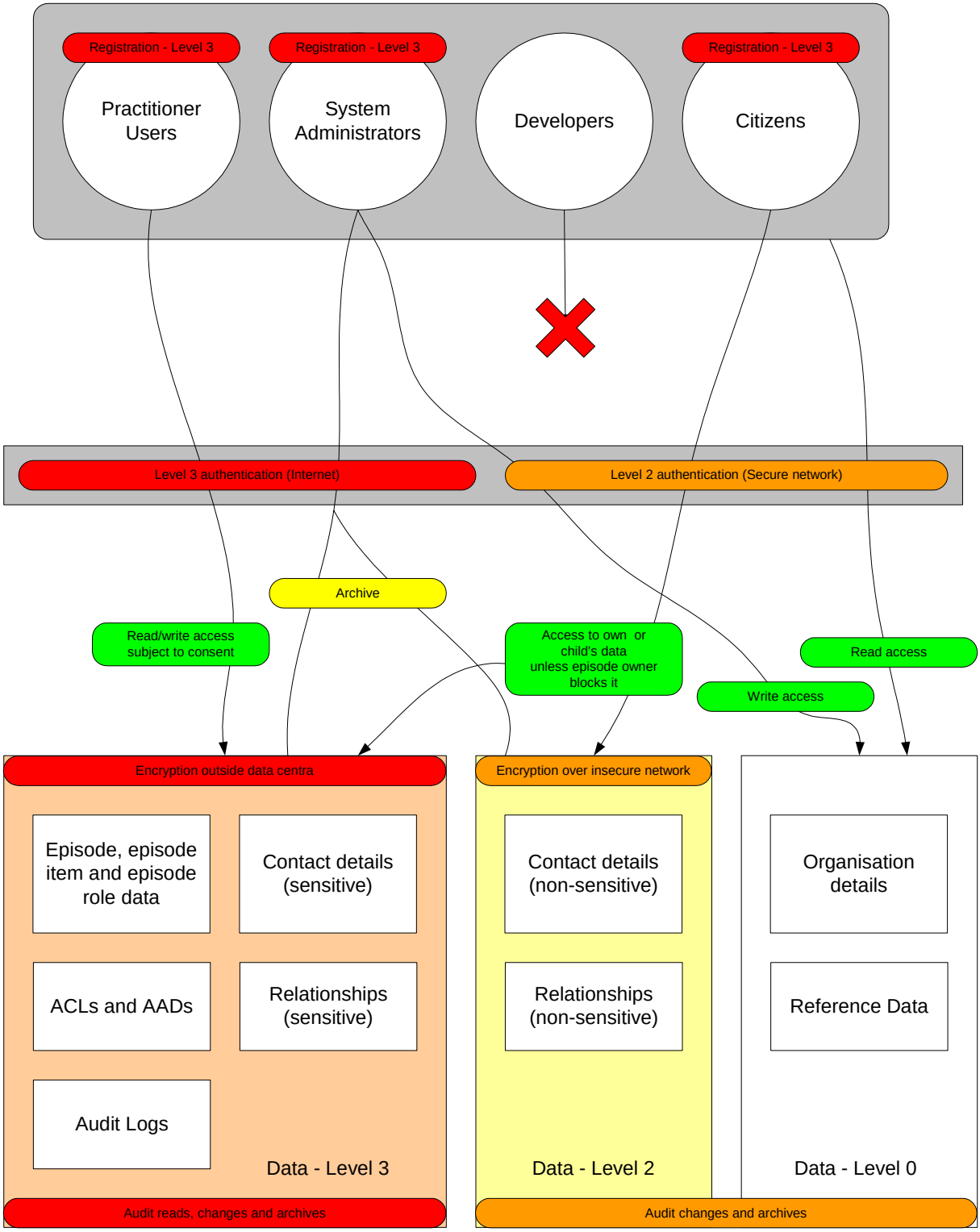


Figure 5-1 Security Policy Summary

6. Interoperability and Usability

In this chapter we discuss measures that can be taken to minimise the overhead of registering, administering and authenticating users. The aim in all cases is to allow these overheads to be shared between organisations, thereby minimising duplication of effort and unnecessary cost.

Note that this section is for guidance only.

The previous sections define security requirements - but the precise technical solution to these requirements is dependant on local infrastructure and out of scope for this document.

It will also be important to monitor the progress of other Every Child Matters initiatives, for example the IS Index. As these projects move towards technical design they too will define requirements and recommendations for security – and it will be important to maintain a compatible approach.

6.1 Single Registration

Chapter 4 specifies standards for checking identities and statuses before giving access to an eCAF implementation.

The checking can be performed by the eCAF operator from scratch (and this will always need to be done for personal users).

Sponsored users may, however, be bulk-registered by their sponsoring organisation. For this to be done, the sponsoring organisation must itself have its identity checked at level 3 and its procedures for checking new staff must meet the requirements of this security architecture. In effect, the registration process is being delegated to the sponsoring organisation.

In many cases, a child or carer will be known to a practitioner when an assessment is made and it would be unnecessary to perform a full registration check at that time. It is also inadvisable to create an air of distrust by demanding full registration in every case. Therefore, the appropriate level of identity checking required is best left to the judgment of the individual practitioner. Occasions where identity checks are more likely to be appropriate include:

- Where a child or carer moves from one jurisdiction to another and is not known in the new jurisdiction.
- Where a new actor with a claimed relationship to an episode (say, an estranged parent), asks for information about it.

6.2 Single Administration

Much of the actor-related information in an eCAF implementation will be a duplicate of other information already held and maintained elsewhere. For instance:

- Contact details. This is likely to exist in HR and contact management systems.
- User ID and credential (the password, certificate or token the user uses to logon). This is likely to exist in desktop and network security directories.

- Role, relationship and membership information. This may exist in HR or security databases.

eCAF implementations will in many cases wish to limit duplication and double-entry of data. Here are some possible options:

- Central administration (this is the basic case). eCAF administration is done by a central eCAF team based on user requests. eCAF administration is separate from desktop or other application administration. This option is the simplest to set up but has operational disadvantages, in particular:
    - Keeping actor-related information up to date will be costly and data quality will suffer.
    - Users will have to manage multiple credentials which will result in cost overheads and a low overall level of security.
    - Where eCAF is being accessed by users in many organisations, complex communication links will have to be set up so that requests and responses can be passed between organisations. Checking the origin of requests will create an additional overhead.

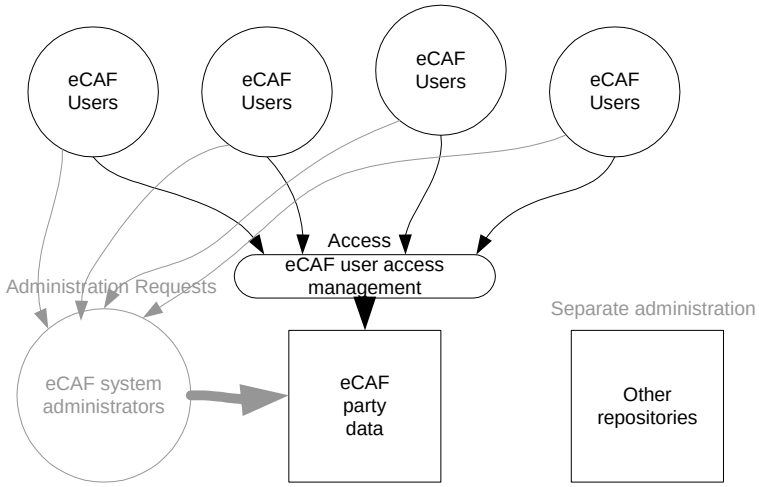


Figure 6-1 Central Administration

- Delegated eCAF administration. Administration is done by a central eCAF team independent of desktop and application administration. However, the central eCAF team can delegate administrators in other organisations who will manage the users and parties within their organisation. This resolves some of the inter-organisation issues of central eCAF administration and is well supported by common user administration applications.

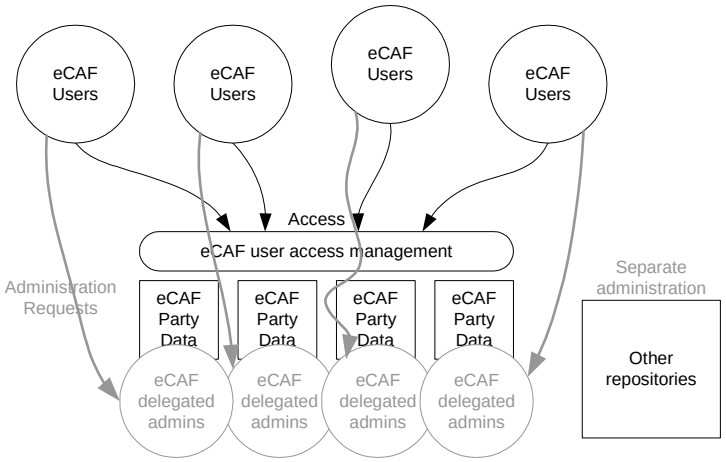


Figure 6-2 Delegated Administration

- Repository synchronization. Each organisation that uses eCAF will continue to maintain its user and party repositories as it does now. Each organisation will arrange for its repositories to be synchronized with the eCAF repositories (periodically, or when a change is made). This keeps eCAF up to date automatically and removes the user problem of managing multiple credentials. However it can be complex to set up securely and requires a high level of trust between the organisations involved.

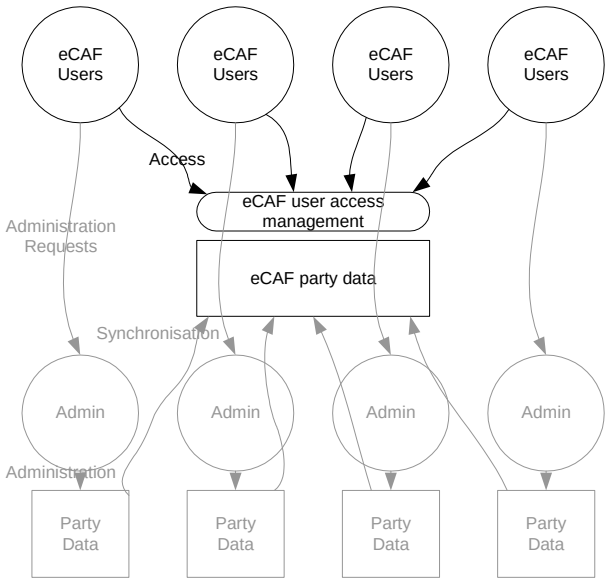


Figure 6-3 Repository Synchronisation

- Virtual repository. Each organisation that uses eCAF will continue to maintain its user and party repositories as it does now. The eCAF application will be configured to understand how to retrieve the information it needs from all of these repositories. Again, this can require complex configuration and will rely upon the performance of the underlying repositories.

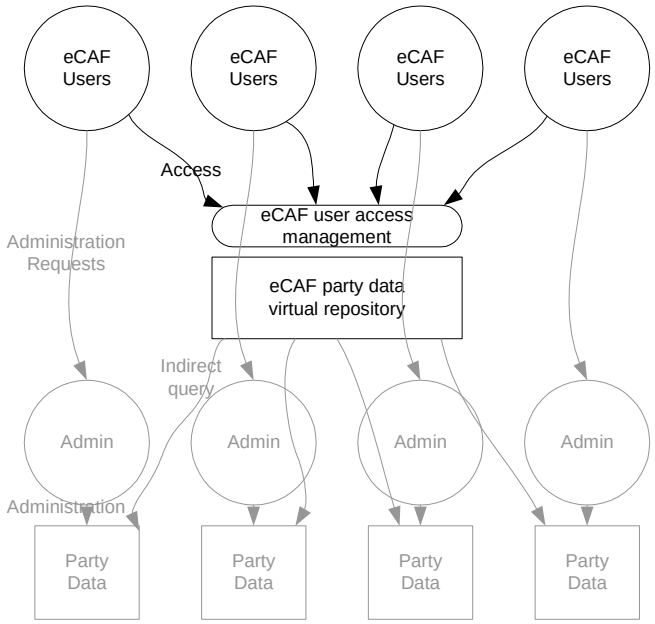


Figure 6-4 Virtual Repository

- Federation. Each organisation that uses eCAF will continue to maintain its user and party repositories as it does now. Whenever a user makes a request, the user agent will send the request to eCAF along with enough information to allow eCAF to authenticate him and make access decisions (in practice, the user agent will usually engage in a secure dialog to do this). This is in many ways the best solution but the technology to implement the idea securely is highly immature.

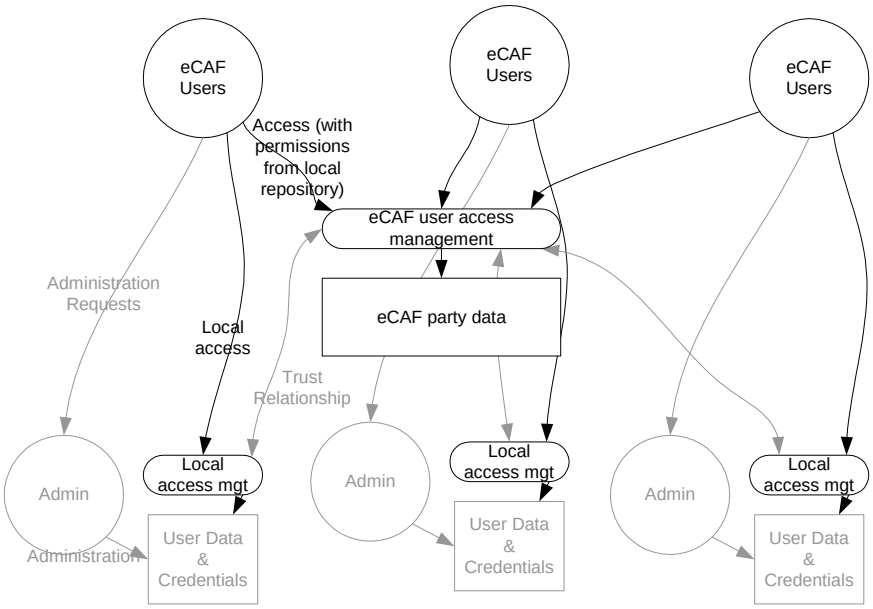


Figure 6-5 Federation

A single eCAF implementation may use different approaches with different attributes, or different user organisations.

It is possible for eCAF implementations to share user repositories, thereby producing a single repository which is used by several different implementations. In this case, all the issues and options described still apply.

It is important that, where a master repository is being synchronized to a slave, the master must meet all the security requirements for the slave. For instance, the master must meet at least as high a registration and authentication level as the slave.

6.3 Single Sign-on

Organisations are increasingly seeing a need to reduce the number of times a user needs to logon during a typical working day. Practical schemes to achieve this include:

- Session federation. This involves sharing session information between applications or organisations using one of the schemes outlined in Section 6.2 (in most cases using the Federation scheme). Again, the producer of session information must be working to at least as high a security level (measured by registration and authentication levels) as the slave.
- Backend data synchronization. If eCAF instances share data to the extent that they can give their users a full picture of what is happening in their area, then this will lessen the requirement for single sign-on.
- Wallets. These store credentials for numerous applications on a user's workstation, and understand how to 'impersonate' the user's role in logging on to each application. These do not handle credential changes well, and can create integration and security problems; for this reason they are strongly deprecated for eCAF.

6.4 Service Providers

eCAF implementations can considerably simplify addressing the issues discussed above by using an existing access management service. In effect, this outsources some proportion of the registration, administration and authentication task to the service.

This paper will consider the following services:

- Eduserve Athens.
- GovConnect.
- CJIT.

The table below lists the services side by side for comparison.

Access Management Service Comparison (As at Nov 2005)			
	Athens	GovConnect (separate services for citizens and employees).	CJIT
Managed by	Eduserve	DCA, supported by Bolton MBC	Home Office
Timescales	Exists	Probably 2006	Live by June 2006
Existing user Populations	3.5M in education and health	Citizens: several million. Employees: none.	450K in police, courts and young offender organisations.
Registration Services	Identity checks not performed.	Citizens: Govconnect will perform L1 identity check. Employees: LA would perform identity checks.	Identity checks delegated to member organisations.
Administration Services	Classic Athens supports delegated administration. AthensDA supports repository synchronization. Athens Shibboleth supports federation through a SAML profile.	Citizens: self service only. Employees: GovConnect would provide a root credential to the LA which would in turn administer its users locally. GovConnect may provide tools to assist LAs. Not certain whether non-LAs will be supported.	Delegation and federation will be supported.
Authentication Services	Included. AthensDA provides a proprietary SSO service and Athens Shibboleth provides a standardized SSO service.	Citizens: User authentication supported. Employees: authentication is by exchanging signed XML messages.	Included. SSO is by LTPA cookie and federation.

Access Management Service Comparison (As at Nov 2005)			
	Athens	GovConnect (separate services for citizens and employees).	CJIT
Standards Support	Proprietary, SAML	XML signature or SAML (TBD).	LTPA, LDAP, SAML, WS-*
Token Support	In planning phase.	In planning phase.	Will be available over Internet.
Connectivity Required	Internet.	Citizens: Internet. Employees: GCSX, should be accessible to 100% of LAs	Internet, GSI, GSX or CJX
Cost	Each eCAF instance costs £1500 one-off and must pay £100 per accessing organisation. Each user organisation must pay £450/year for up to 100 users and £2 per user per year for each additional user.	Unknown.	TBD
Security	Athens is aimed at the lower security levels (level 1 on our scale).	L1 today. L2/3 sometime in the future.	Aimed at the RESTRICTED protective marking (equivalent to Level 3 on our scale)

Note that the situation regarding these service providers is evolving quickly. The information in the table above is provided for guidance and to indicate the kind of services available. However it is likely to go out-of-date and, in particular, GovConnect is currently undergoing a process of revision and change. It is recommended to check the latest situation and monitor on an ongoing basis.