

MANUAL

DATA ACQUISITION & CONTROL ARCHITECTURE (DACA) – TECHNICAL CONTROLS – AUTHENTICATION AND AUTHORISATION

DEP 32.01.23.15-Gen.

June 2007

DESIGN AND ENGINEERING PRACTICE



This document is restricted. Neither the whole nor any part of this document may be disclosed to any third party without the prior written consent of Shell Global Solutions International B.V., The Netherlands. The copyright of this document is vested in this company. All rights reserved. Neither the whole nor any part of this document may be reproduced, stored in any retrieval system or transmitted in any form or by any means (electronic, mechanical, reprographic, recording or otherwise) without the prior written consent of the copyright owner.

PREFACE

DEPs (Design and Engineering Practice) publications reflect the views, at the time of publication, of:

Shell Global Solutions International B.V. (Shell GSI)

and/or

Shell International Exploration and Production B.V. (SIEP)

and/or

other Shell Service Companies.

They are based on the experience acquired during their involvement with the design, construction, operation and maintenance of processing units and facilities, and they are supplemented with the experience of Shell Operating Units. Where appropriate they are based on, or reference is made to, international, regional, national and industry standards.

The objective is to set the recommended standard for good design and engineering practice applied by Shell companies operating an oil refinery, gas handling installation, chemical plant, oil and gas production facility, or any other such facility, and thereby to achieve maximum technical and economic benefit from standardization.

The information set forth in these publications is provided to Shell companies for their consideration and decision to implement. This is of particular importance where DEPs may not cover every requirement or diversity of condition at each locality. The system of DEPs is expected to be sufficiently flexible to allow individual Operating Units to adapt the information set forth in DEPs to their own environment and requirements.

When Contractors or Manufacturers/Suppliers use DEPs they shall be solely responsible for the quality of work and the attainment of the required design and engineering standards. In particular, for those requirements not specifically covered, the Principal will expect them to follow those design and engineering practices which will achieve the same level of integrity as reflected in the DEPs. If in doubt, the Contractor or Manufacturer/Supplier shall, without detracting from his own responsibility, consult the Principal or its technical advisor.

The right to use DEPs is granted by Shell GSI, in most cases under Service Agreements primarily with Shell companies and other companies receiving technical advice and services from Shell GSI or another Shell Service Company. Consequently, three categories of users of DEPs can be distinguished:

- 1) Operating Units having a Service Agreement with Shell GSI or other Shell Service Company. The use of DEPs by these Operating Units is subject in all respects to the terms and conditions of the relevant Service Agreement.
- 2) Other parties who are authorized to use DEPs subject to appropriate contractual arrangements (whether as part of a Service Agreement or otherwise).
- 3) Contractors/subcontractors and Manufacturers/Suppliers under a contract with users referred to under 1) or 2) which requires that tenders for projects, materials supplied or - generally - work performed on behalf of the said users comply with the relevant standards.

Subject to any particular terms and conditions as may be set forth in specific agreements with users, Shell GSI disclaims any liability of whatsoever nature for any damage (including injury or death) suffered by any company or person whomsoever as a result of or in connection with the use, application or implementation of any DEP, combination of DEPs or any part thereof, even if it is wholly or partly caused by negligence on the part of Shell GSI or other Shell Service Company. The benefit of this disclaimer shall inure in all respects to Shell GSI and/or any Shell Service Company, or companies affiliated to these companies, that may issue DEPs or require the use of DEPs.

Without prejudice to any specific terms in respect of confidentiality under relevant contractual arrangements, DEPs shall not, without the prior written consent of Shell GSI, be disclosed by users to any company or person whomsoever and the DEPs shall be used exclusively for the purpose for which they have been provided to the user. They shall be returned after use, including any copies which shall only be made by users with the express prior written consent of Shell GSI. The copyright of DEPs vests in Shell GSI. Users shall arrange for DEPs to be held in safe custody and Shell GSI may at any time require information satisfactory to them in order to ascertain how users implement this requirement.

All administrative queries should be directed to the DEP Administrator in Shell GSI.

TABLE OF CONTENTS

1.	INTRODUCTION	4
1.1	SCOPE.....	4
1.2	DISTRIBUTION, INTENDED USE AND REGULATORY CONSIDERATIONS	4
1.3	DEFINITIONS	4
1.4	ABBREVIATIONS	5
1.5	CROSS-REFERENCES	6
1.6	COMMENTS ON THIS DEP	6
2.	GENERAL PRINCIPLES	7
2.1	FRAMEWORK	7
2.2	ACCOUNTABILITY VERSUS GROUP ACCOUNTS	9
2.3	AUTHENTICATION PRINCIPLES IN THE PCD	9
2.4	PRIVILEGES TO PCD SYSTEMS.....	9
3.	AUTHENTICATION	11
3.1	GENERAL	11
3.2	FEASIBILITY AND DEPLOYABILITY	11
3.3	AUTHENTICATION LEVEL	11
3.4	GRANULARITY AND EXTENSIBILITY	11
4.	IMPLEMENTING AUTHORISATION PROCEDURES	12
4.1	GENERAL	12
4.2	CONTROLLING LOGON TO PARTICULAR SYSTEMS.....	12
4.3	SETTING LOGON HOURS	12
4.4	APPLYING PRINCIPLE OF LEAST PRIVILEGE	12
4.5	ENFORCING SECURITY AUDIT POLICY	13
5.	PASSWORD GUIDELINES	15
5.1	GENERAL	15
5.2	VULNERABILITIES AND PREVENTION METHODS	15
6.	REFERENCES	18

1. INTRODUCTION

1.1 SCOPE

This new DEP specifies requirements and gives recommendations for the implementation of secure authentication and authorisation to be used on all systems and applications in the Process Control Domain (PCD) and the Process Control Access Domain (PCAD). This DEP does not apply to the Office Domain.

The purpose of this DEP is to provide guidance to Operating Units on the implementation of authentication and authorisation.

This DEP supports ITCI 117.

This DEP is primarily intended for:

- PCD Administrators;
- PCAD Administrators;
- Vendors;
- Engineering consultants.

1.2 DISTRIBUTION, INTENDED USE AND REGULATORY CONSIDERATIONS

Unless otherwise authorised by Shell GSI, the distribution of this DEP is confined to Shell companies and, where necessary, to Contractors and Manufacturers/Suppliers nominated by them.

This DEP is intended for use in major development projects and existing producing assets in exploration and production. However, it may be applied to other Business Groups at the discretion of the Principal.

When DEPs are applied, a Management of Change (MOC) process should be implemented; this is of particular importance when existing facilities are to be modified.

If national and/or local regulations exist in which some of the requirements may be more stringent than in this DEP, the Contractor shall determine by careful scrutiny which of the requirements are the more stringent and which combination of requirements will be acceptable with regards to the safety, environmental, economic and legal aspects. In all cases the Contractor shall inform the Principal of any deviation from the requirements of this DEP which is considered to be necessary in order to comply with national and/or local regulations. The Principal may then negotiate with the Authorities concerned, the objective being to obtain agreement to follow this DEP as closely as possible.

1.3 DEFINITIONS

1.3.1 General definitions

The **Contractor** is the party that carries out all or part of the design, engineering, procurement, construction, commissioning or management of a project or operation of a facility. The Principal may undertake all or part of the duties of the Contractor.

The **Manufacturer/Supplier/Vendor** is the party that manufactures or supplies equipment and services to perform the duties specified by the Contractor.

The **Principal** is the party that initiates the project and ultimately pays for its design and construction. The Principal will generally specify the technical requirements. The Principal may also include an agent or consultant authorised to act for, and on behalf of, the Principal.

The word **shall** indicates a requirement.

The word **should** indicates a recommendation.

1.3.2 Specific definitions

Authentication and authorization each have a very specific meaning, although the two processes are often confused with each other, and in practice often not clearly distinguished. In this DEP the term "access management" is used to describe broader systems that may make use of both authentication and authorization services in order to control use of a networked resource.

Authentication The process whereby a network user establishes a right to an identity, in essence, the right to use a name. There are a large number of techniques that may be used to authenticate a user: passwords, biometric techniques, smart cards, and certificates. Names need not correspond to the usual names of individuals. A user may have the rights to use more than one name. On the other hand the name only belongs to one unique user.

Authorization The mechanism by which a system determines what level of access a particular authenticated user should have to secure resources controlled by the system.

NOTES: 1. Permission to perform an action does not guarantee that the action can be performed; for example, a common practice in authorization is to further limit access to a maximum number of concurrent users from among an authorized user group.

2. Authentication and authorization decisions can be made at different points, by different organizations.

Two-factor authentication A security process in which the user provides two means of identification, one of which is typically a physical token, such as a card, and the other of which is typically something memorized, such as a security code. In this context, the two factors involved are sometimes spoken of as something you have and something you know.

1.4 ABBREVIATIONS

CCR	Central Control Room
DACA	Data Acquisition and Control Architecture
DCOM	Distributed Component Object Model
GI	Shell Group Standard for Global Infrastructure
GID	Global Infrastructure Desktop
GIH	Global Infrastructure Hosting
GPO	Group Policy object
IPS	Instrumented Protective System
ITCI	Group IT Security Office
MOB	Mobile Office Business
MOP	Mobile Office Private
NTFS	NT File System
OD	Office Domain
OLE	Object Linking and Embedding
OPC	OLE for Process Control
PCAD	Process Control Access Domain
PCD	Process Control Domain
PCDP	Process Control Domain Portal
PCN	Process Control Network
RTU	Remote Telemetry Unit
TD	Trust Domain
TPA	Third Party Access

1.5 CROSS-REFERENCES

Where cross-references to other parts of this DEP are made, the referenced section number is shown in brackets. Other documents referenced by this DEP are listed in (6).

1.6 COMMENTS ON THIS DEP

Comments on this DEP may be sent to the DEP Administrator at standards@shell.com. Shell staff may also post comments on this DEP on the Surface Global Network (SGN) under the Standards folder.

2. GENERAL PRINCIPLES

2.1 FRAMEWORK

The framework for authentication is based on providing several layers of protection to verify that a user is the person he claims to be. It consists of two independent characteristics, which are often complementary.

One layer of protection is based on the complexity of the verification used in the log-on screens of systems and applications.

The other layer of protection is based on the physical barriers a person needs to penetrate before he can get physical access to a system. For instance, a CCR operator who is at a workstation that is located on an offshore platform has to pass several barriers to get there. He does not need to log on to the workstation each time he wants to access it.

On the other hand, logging on to a workstation on a normally unmanned facility in the desert will require some form of two-factor authentication since there is little certainty about the identity of that user. It could be an intruder.

Strict controls on one aspect of authentication could allow some relaxation of the other aspect of authentication, as is described in the following figure and the tables below.

For details on the remote and local aspects and how these should be interpreted, refer to DEP 32.01.23.12-Gen.

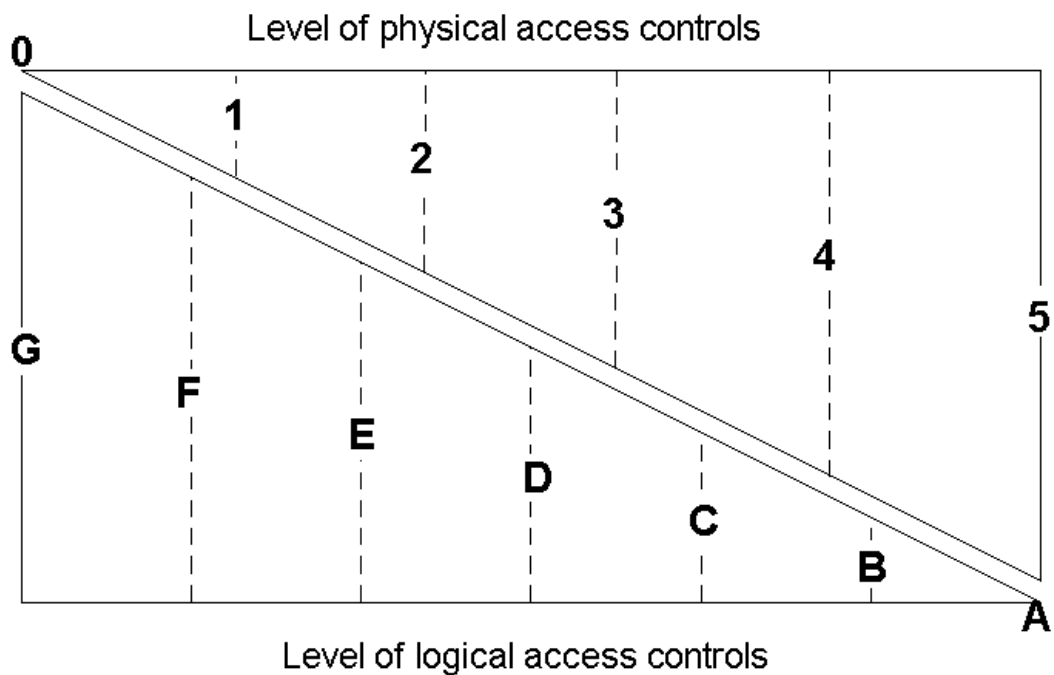


Figure 1 Complementing logical and physical access controls

Table 1 Level of logical access controls

	Description	Example
A	No authentication	No username, no password required
B	Username only	No password required
C	One-factor, group account	General account with shared password
D	One-factor, personal account	Personal account with personal password
E	Two-factor	Password based on the principle of something you have and something you know (e.g. smartcard with PIN) See Note (1)
F	One-factor plus hardware key / switch	Personal account with personal password, which is only accepted when a key is turned or a switch is operated
G	Two-factor plus hardware key / switch	Password based on the principle of something you have and something you know (e.g. smartcard with PIN), which is only accepted when a key is turned or a switch is operated
NOTE: For the purposes of authentication and authorization in the PCD, "two-factor" can mean a combination of physical and electronic controls. For example, access to a control system on a gas plant may be restricted via gate access controls plus login/password.		

For a number of locations from which the system can be accessed, certain assumptions have been made about the levels of physical access controls, as summarised in Table 2.

Table 2 Levels of physical access controls

	Description	Example
0	Outside the control of the company	Third Party Access
1	Normally unmanned, physically uncontrolled	RTU on a wellsite without fences
2	Within the controlled OD	Remote client
3	Normally unmanned, physically controlled	Field Auxiliary Room within protected, fenced area and locked doors. Operator only occasionally present.
4	Normally manned, physically uncontrolled	Normally daytime manned facility but no permanent presence. Typically a remote production facility with daytime operator attendance. Fenced and locked.
5	Continuously manned, physically controlled	Normally 24/7 manned facility, guard or operator always present. For instance a CCR.

Table 3 specifies the minimum security requirements that consist of both physical security and log-on security. Operating units may amend this table to reflect local conditions.

Table 3 Minimum security requirements

			Type of security requirement			
			Monitoring	Control	IPS	Admini- stration
Location	Local		E1 / E3 / C4	E3	F/G	E1
	REMOTE	CCR / Level 3	A5	A5	F/G	E5
		PCN / Level 3	C4 / D3	C4	F/G	E3
		Office / Level 4	E2	X	X	E2
		TPA / Level 5	E0	X	X	E0

The level of logical access controls for an IPS is independent of the physical access controls present at that location. ITCI 117 section 4.6 specifically requires a local switch at the IPS to enable configuration changes. The only means of logical access to the IPS will be through an Engineering Work Station connected to the Level 2 network or a safety bus.

Example: If a maintenance technician requires access to a system for wellhead monitoring, for instance to see live I/O from a workstation on the Process Control Network (PCN), there are two options:

- For a normally daytime manned facility without permanent presence, for instance a remote production facility with daytime operator attendance only (physical access control level 4), he can use a group account using one-factor authentication (authentication level C).
- If he requires this access in a Field Auxiliary Room without continuous operator presence (physical access control level 3) he can only get access using a personal account (authentication level D).

If he connects locally to the field device, for instance an RTU (physical access control level 1), he must use two-factor authentication (authentication level E). This may consist of login/password, plus keyed access to a locked cabinet.

2.2 ACCOUNTABILITY VERSUS GROUP ACCOUNTS

Accountability and the use of group accounts are incompatible. With group accounts and without physical controls accountability is not possible.

For instance, if an operator logs on to his workstation as a SHIFT1 group user he will have some kind of privacy since his identity cannot be tracked back from the log files. His shift may consist of a supervisor and a number of shift operators. In that case, the supervisor will be accountable for all the actions of his shift.

That practice may not be acceptable in all cases and this should be taken into account when assigning group accounts. Additional controls should be in place, such as duty roster, permit to work, etc. The Operating Unit Engineering Manager shall specifically approve the use of group accounts.

ITCI 117 Section 4.4.11: *Every node within the PCD/ PCAD that routes network traffic must be explicitly authorised to do so by a designated point of authority.*

This last authority or person takes the full accountability for that traffic.

2.3 AUTHENTICATION PRINCIPLES IN THE PCD

The PCD environment shall have an autonomous authentication mechanism. For instance, in a Windows environment this means there shall be no trust relationship with the Shell Group Infrastructure (GI) or other domains in the OD.

ITCI 117 Section 4.4.1: *All access to the PCD including applications and system administration via the PCAD must be controlled by one or other of the following as a minimum:*

- *Two-factor authentication*
- *One time password.*

ITCI 117 Section 4.4.8: *Each system or user that connects to a PCD from outside a Shell TD network via the PCAD shall only be permitted to do so based on need and requires approval of a designated single point of authority.*

2.4 PRIVILEGES TO PCD SYSTEMS

User access to applications in the PCD shall be kept to a minimum. In many cases the user access need can be transferred to the OD by making use of Plant Information (product of OSI-Soft) or by a restructuring of the applications.

- Only the PCD administrator or persons specifically authorised by the PCD administrator shall have the credentials for the administrator or root password of systems.
- User access to specific application that allows changes to the configuration shall always be a named person, or at least traceable to a named person.
- A user should only get access to systems if there is a clear business need.

3. AUTHENTICATION

3.1 GENERAL

There are trade-offs that will need to be made between the conflicting goals in each specific resource access arrangement, and users of this DEP will need to make policy choices about the relative importance of the various requirements.

3.2 FEASIBILITY AND DEPLOYABILITY

First and foremost, the authentication and access management solution needs to work at a practical level. From the user's perspective, it should facilitate access, minimize redundant authentication interactions and provide a single sign-on, user-friendly view of the available networked information resources. It shall be usable and manageable in practical terms. It shall be sufficiently robust and simple so that user support issues are traceable; for example, a forgotten password should not be a big problem.

Single Sign-On (SSO) is the mechanism whereby a single action of user authentication can permit a user to access all computers and systems for which he has access permission, without the need to enter multiple passwords or other credentials.

3.3 AUTHENTICATION LEVEL

The system shall ensure that an attacker cannot forge a credential. All parties need to be confident that credentials cannot be stolen by eavesdroppers on the net (for example, through sniffer attacks), and that they cannot be stolen from a user taking the proper precautions. Also, system compromise is a concern: there is a big difference between an individual user's credentials being compromised (in which case they can be cancelled and new ones issued) and the system as a whole being compromised, which might need credentials to be re-issued to all users.

The "strength" of authentication is largely a matter of subjective interpretation. For many approaches, strength depends on the cryptographic algorithms and the key lengths used, and partly on the overall system design and implementation, and on actual user behaviour, which can often be the source of the largest number of vulnerabilities. Reasonable judgement is required: for most of the resources subject to access control, no immediate safety or security risks will arise if access control is breached. An access management system needs to be complemented by monitoring and other controls on the part of the PCD administrator to limit the impact of a breach. Further, after-the-fact legal remedies may be available to limit the damage caused by such a breach.

The mechanism of two-factor authentication, where required, shall be agreed upon for each PCD.

3.4 GRANULARITY AND EXTENSIBILITY

"Fine-grained" access control shall be applied if resource access is to be limited to only certain groups or individuals or to certain parts of the resource. For example, certain users may be allowed to change some data or structure in the historian, while other users are only allowed to read data or parts of data.

4. IMPLEMENTING AUTHORISATION PROCEDURES

4.1 GENERAL

Wherever possible, access to systems within the PCD should be granted on the basis of unique accounts that are traceable (e.g. can be traced to a specific user or service). Maintaining unique and traceable accounts ensures that the account cannot be misused, either by allowing unauthorized access to the account itself and the privileges the account holds, or by permitting any account to elevate its privileges in order to access systems that the account is unauthorized to access.

This section discusses the following examples for the implementation of secure authorisation:

- Controlling which systems an account may logon to
- Controlling what time of day and which days of the week an account may be used
- Applying principle of least privilege
- Enforcing security audit policy

4.2 CONTROLLING LOGON TO PARTICULAR SYSTEMS

Some network directories like Microsoft Domains or Active Directory enable an account to be restricted in such a way that it can only be used on specific member systems of that directory (or domain for Windows). This can be used as one of the ways to implement the least privilege principle.

4.3 SETTING LOGON HOURS

Some systems enable the restricting of access to a system to particular days or times of day. This can also be a useful way to support the least privilege principle. For instance:

- Operator: 24x7
- Office user: 8x5
- Third parties: as defined in a Service Level Agreement

Using the restriction of logon hours should be considered carefully as lifting or loosening the restriction might not be possible at short notice. On some systems, if a user is currently logged on, such changes will not take effect until the user logs off and back on again.

4.4 APPLYING PRINCIPLE OF LEAST PRIVILEGE

ITCI 117 Section 4.1.5: *Access rights, permissions, and privilege levels shall be minimal, time dependent, role-dependent and named user specific. Group accounts shall only be applied at the discretion of the Operating Unit Engineering Manager.*

Application of the principle of least privilege ensures that users cannot access systems beyond what is approved, and that the user of an account cannot elevate the privileges the account holds without intervention by the systems administrator.

Consequently, any accounts outside (not a member of) the 'Administrators' group shall not be permitted to modify the privileges an account holds, including the ability to:

- Modify (add, change, or delete) accounts
- Modify local or domain policy
- Clear System, Application, or Security event logs
- Modify User rights assignments

Several examples of common measures which limit authorisations and are taken to ensure minimal access are given below. The functionality of a system may be impacted severely by these and similar measures. They shall be tested and, where applicable, approved by Vendors before implementation.

In the NTFS file system on Windows 2000: the default access to all file system objects is 'EVERYONE - FULL CONTROL'. This permits anyone, local or domain, to take complete control over a file system and must therefore be further restricted. Each NTFS file system should be configured as follows.

- Open the disk properties page and use the 'Security' tab to configure file permissions.
- The 'Everyone' group should be removed, and replaced with the 'Administrators', 'SYSTEM', 'Power Users', 'Users', and 'Backup Operators' groups.
- The 'Administrators' and 'SYSTEM' groups should be granted full control, which includes read, write, list folder contents, execute, and the ability to change group permissions.
- The 'Power Users' group should be granted read, write, list folder contents, and execute permissions.
- The 'Users' and 'Backup Operators' groups should be granted only the permission to read, list folder contents, and execute.
- When these permissions are applied, they should be applied at the root level of the drive and then be propagated to sub folders and files through inheritance.
- Once these groups have been established with the appropriate permissions, each group's membership should be reviewed to ensure each member account indeed has the proper level of authority.
- Similar permissions schemes exist for access to DCOM components. Where OPC servers are installed, use the Windows 'DCOMCNFG' utility to grant permissions to access and/or launch, or configure permissions for OPC servers. The 'Everyone' group shall be specifically removed from these permissions sets and accounts or groups which should have access to an OPC server shall be explicitly defined.

4.5 ENFORCING SECURITY AUDIT POLICY

As part of ensuring the ability to trace a user account, Windows provides a security audit trail. On Windows systems all security auditing is disabled by default; therefore both success and failure based security event auditing should be enabled.

As an example this is how to enable security auditing functionality on Windows 2000:

- To configure the security event log settings, use the default domain policy. Logon to the PCD domain controller and open the Domain Security Policy console (**START→Programs→Administrative Tools→Domain Security Policy**).
- In the Policy snap-in, under **Windows Settings**, double-click **Security Settings**, double-click **Local Policies**, and then select **Audit Policy**.

Both the success and failure for the following events should be audited:

- Account Logon Events
 - Process tracking
 - Privilege Use
 - Object Access
 - Logon Events
 - System Events
 - Directory Service Access
 - Account Management
 - Policy Change
- To ensure the security event log sub-systems can provide an adequate container for hosting security events:
 - Set the maximum-security log size to 10,000 KB or more. This helps to ensure that important events are not overwritten when the log file becomes large in size.
 - Set the event retention method to Overwrite events as needed
 - Disable the computer from shutting down if the event log becomes full
 - Restrict Guest level access to the Event log
- To configure the security event log settings, use the default domain policy. Logon to the PCD domain controller and open the Domain Security Policy console (**START→Programs→Administrative Tools→Domain Security Policy**).
- In the Policy snap-in, under **Windows Settings**, double-click **Security Settings**, double-click **Event Log**, and then select **Settings for Event Log**.
- A central repository for collecting events should be established, using suitable tools. These tools may help to prevent important events from being overwritten or deleted, and can help to ensure that log data is retained to comply with local or regulatory requirements.

5. PASSWORD GUIDELINES

5.1 GENERAL

In order to authenticate a user, some kind of proof is required in order to be sure that the user is who he claims to be. Requiring user passwords is a common method in implementing authentication.

One of the threats to authentication is identity theft. There always exists a threat that passwords are revealed and used to impersonate another user. This threat can be exploited by several vulnerabilities, among which are password discovery, password interception and social engineering.

5.2 VULNERABILITIES AND PREVENTION METHODS

5.2.1 Overview

Table 5 gives an overview of the vulnerabilities and prevention related to the threat of identity theft.

Table 5 Overview of vulnerabilities and prevention methods

Vulnerabilities related to impersonation threat	
Vulnerability	Prevention
1. Password discovery	- Use strong password - Change default passwords - Use one-time passwords - Awareness training - Hardening
2. Password interception	- Use one-time passwords - Encryption of passwords
3. Social Engineering	- Awareness training

5.2.2 Methods for mitigation

5.2.2.1 General

For each of these vulnerabilities, there are multiple methods for mitigation. Table 5 shows the method that can be used to mitigate each vulnerability.

5.2.2.2 Password complexity for strong passwords

Passwords can be made stronger by increasing the length and/or raising the complexity of the password.

Password complexity always has to be seen in relation with the expiration time, the current (or future) computational possibilities, the business criticality and the other mitigations implemented.

ITCI 117 Section 4.4.4: *For every application and system inside the PCD the use of strong passwords is required. A strong password must contain characters from three of the four character sets:*

- *Lowercase*
- *Uppercase*
- *At least one numeric digit*
- *At least one special character (% , # , etc)*
- *8 positions*

5.2.2.3 Password Age

Password age is the length of time an account can be used before the password must be changed.

ITCI 117 Section 4.4.6: *Users shall be prompted to change their passwords within 30 days of expiration. After these 30 days have expired without user intervention, the account will require a reset by the PCD administrator (with the exception of service, auto login and operator accounts)*

5.2.2.4 Account expiration

Account expiration is a mitigation that prevents an account that has been unused for a certain time from further being used. Systems may be configured to enforce account expiration by blocking the account after a number of days/months without usage.

ITCI 117 Section 4.4.5: *Local and Domain User Account passwords shall be configured to expire automatically and be reset every 180 days, with the exception of service, auto-login and operator accounts, which shall never expire automatically.*

5.2.2.5 Password history

Password history is a mitigation that prevents a user from reusing a previous password. Systems may be configured to enforce password history, anywhere from zero to several previously used passwords.

Wherever possible, the password history should be enabled.

5.2.2.6 One-time passwords

The purpose of a **one-time password** (OTP) is to make it more difficult to gain unauthorized access to restricted resources like a computer account, by disabling the re-use of a captured password. This is an example of another mitigation that opens the possibility to lower the complexity requirement for a password.

5.2.2.7 Password security

A password should be protected from discovery while stored on disk and during transmission. This is achieved by using encryption and hashing techniques. Plaintext passwords shall not be used.

5.2.2.8 Multiple Login restriction

Multiple login restriction is a mitigation that prevents a user from using the same user on different systems at the same time. This actively prevents an account from being abused while the legitimate user is working on any other system.

5.2.2.9 Login retries

ITCI 117 Section 4.4.2: *For user access to the PCAD: After 3 consecutive failed authentication login attempts, accounts shall be blocked and may only be unlocked by administrators.*

ITCI 117 Section 4.4.3: *For user access to systems within the PCD: After 25 consecutive failed authentication login attempts, accounts shall be blocked and subsequently automatically unblocked after 5 minutes. Special user accounts such as Operator accounts should never be blocked.*

5.2.2.10 Exceptions

Exceptions to this baseline are service, auto-login and operator accounts, which shall never be blocked automatically.

6. REFERENCES

In this DEP, reference is made to the following publications:

- NOTES:
1. Unless specifically designated by date, the latest edition of each publication shall be used, together with any amendments/supplements/revisions thereto.
 2. The DEPs and most referenced external standards are available to Shell staff on the SWW (Shell Wide Web) at <http://sww05.europe.shell.com/standards/>.

SHELL STANDARDS

Data Acquisition & Control Architecture (DACA) – Technical
Controls – Remote user access

DEP 32.01.23.12-Gen.

Information security standard for PCADs and PCDs

ITCI 117