IEC 62351-8

Edition 1.0 2020-04

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Power systems management and associated information exchange – Data and communications security –
Part 8: Role-based access control for power system management

Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données –
Partie 8: Contrôle d'accès basé sur les rôles pour la gestion de systèmes de puissance

IEC 62351-8:2020-04(en-fr)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
67 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

A propos de l'IEC
La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC
Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Recherche de publications IEC - webstore.iec.ch/advsearchform
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,…). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

Service Clients - webstore.iec.ch/csc
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

Electropedia - www.electropedia.org
Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 000 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary
67 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

IEC 62351-8

Edition 1.0 2020-04

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Power systems management and associated information exchange – Data and communications security – Part 8: Role-based access control for power system management

Gestion des systèmes de puissance et échanges d'informations associés – Sécurité des communications et des données – Partie 8: Contrôle d'accès basé sur les rôles pour la gestion de systèmes de puissance

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 33.200

ISBN 978-2-8322-8072-0

CONTENTS

FOREWORD 6
INTRODUCTION 8
1 Scope 9
2 Normative references 10
3 Terms and definitions 11
4 Abbreviated terms 13
5 RBAC process model 14
5.1 Overview of RBAC process model 14
5.2 Generic RBAC concepts 15
5.3 Separation of subjects, roles, and permissions 16
5.3.1 RBAC model 16
5.3.2 Subject assignment (subject-to-role mapping) 18
5.3.3 Role assignment (role-to-permission mapping) 18
5.3.4 Permission assignment (mapping of actions to objects) 19
5.4 Criteria for defining roles 19
5.4.1 Policies 19
5.4.2 Subjects, roles, and permissions 19
5.4.3 Introducing roles reduces complexity 19
6 Definition of roles 20
6.1 Role-to-permission assignment inside the entity in general 20
6.1.1 General 20
6.1.2 Number of supported permissions by a role 20
6.1.3 Number of supported roles 20
6.1.4 Flexibility of role-to-permission mapping 20
6.2 Role-to-permission assignment with respect to power systems 20
6.2.1 Mandatory roles and permissions for IED access control 20
6.2.2 Power utility automation using IEC 61850 23
6.3 Role to permission assignment for specific roles 25
6.3.1 General 25
6.3.2 Encoding specific roles 25
6.3.3 Evaluation context 29
6.4 Role-to-permission assignment with respect to other non-power system domains (e.g. industrial process control) 30
7 RBAC credential distribution using the PUSH model 30
7.1 General 30
7.2 Secure access to an LDAP-enabled repository 31
7.3 Secure access to an identity provider for retrieval of a JWT 31
8 RBAC credential distribution using the PULL model 32
8.1 General 32
8.2 Secure access to an LDAP-enabled repository 33
8.2.1 General 33
8.2.2 PULL model with LDAP 33
8.2.3 LDAP Directory organization 34
8.3 Secure access to the RADIUS-enabled repository 35
8.3.1 General 35
8.3.2 PULL model with RADIUS 35

8.3.3 RADIUS security applying transparent TLS protection 36
8.4 Secure access to the JWT provider 39
9 General application of RBAC access token (informative) 39
9.1 General 39
9.2 Session-based approach 40
9.3 Message-based approach 42
10 Definition of access tokens 42
10.1 General 42
10.2 Supported profiles 42
10.3 Identification of access token 42
10.4 General structure of the access tokens 43
10.4.1 Mandatory fields in the access tokens 43
10.4.2 Mandatory profile-specific fields 43
10.4.3 Optional fields in the access tokens 43
10.4.4 Definition of specific fields 44
10.5 Specific structure of the access tokens 47
10.5.1 Profile A: X.509 Public key certificate 47
10.5.2 Profile B: X.509 Attribute certificate 49
10.5.3 Profile C: JSON Web Token – JWT 52
10.5.4 Profile D: RADIUS token 54
11 Transport profiles 56
11.1 Usage in TCP-based protocols 56
11.2 Usage in non-Ethernet based protocols 57
12 Verification of access tokens 57
12.1 General 57
12.2 Multiple access token existence 57
12.3 Subject authentication 57
12.4 Access token availability 58
12.5 Validity period 58
12.6 Access token integrity 58
12.7 Issuer 58
12.8 RoleID 58
12.9 Revision number 59
12.10 Area of responsibility 59
12.11 Role definition 59
12.12 Revocation state 59
12.13 Operation 59
12.14 Sequence number 59
12.15 Revocation methods 60
12.15.1 General 60
12.15.2 Supported methods 60
13 Conformity 61
13.1 General 61
13.2 Notation 61
13.3 Conformance to access token format 61
13.4 Conformance to access token content 61
13.5 Access token distribution 61
13.6 Role information exchange 62

13.7 Mapping to existing authorization mechanisms 62
13.8 Security events 62
14 Repository interaction for the defined RBAC profiles 62
Annex A (informative) Informative example for specific role definition 64
A.1 Scope of annex 64
A.2 Use case description 64
A.3 XACML definition example 64
A.4 Role description 65
A.5 Permission group description 66
A.6 Permission description 67
A.7 Request syntax for PDP 70
Bibliography 72

Figure 1 – Generic framework for access control 15
Figure 2 – Diagram of RBAC with static and dynamic separation of duty (enhanced version of [ANSI INCITS 359-2004]) 16
Figure 3 – Subjects, roles, permissions, and operations 18
Figure 4 – XACML structure 26
Figure 5 – Schematic view of authorization mechanism based on RBAC 31
Figure 6 – Schematic view of authorization mechanism based on RBAC PULL model 33
Figure 7 – RBAC PULL model using LDAP 34
Figure 8 – RBAC PULL model using RADIUS 36
Figure 9 – RBAC model using OAuth2.0 and JWT 39
Figure 10 – Session based RBAC approach (simplified IEC 62351-4 end-to-end security) 41

Table 1 – List of mandatory pre-defined permissions 21
Table 2 – Pre-defined roles 22
Table 3 – List of pre-defined role-to-permission assignment 23
Table 4 – LISTOBJECTS permission and associated ACSI services 24
Table 5 – Evaluation Context 29
Table 6 – Cipher suites combinations in the context of this document 37
Table 7 – Mandatory general access token components 43
Table 8 – Mandatory profile specific access token components 43
Table 9 – Optional access token components 43
Table 10 – AoR fields and format 46
Table 11 – Mapping between ID and Attribute Certificate 52
Table 12 – Conformance to access token format 61
Table 13 – Conformance to access token distribution 62
Table 14 – Profile comparison 63

Document history

Any person intervening in the present document is invited to complete the table below before sending the document elsewhere. The purpose is to allow all actors to see all changes introduced and the intervening persons.

Any important message to IEC editors should also be included in the table below.

Name of intervening person	Document received		Brief description of the changes introduced	Document sent	
	From	Date		To	Date
Steffen Fries	WG15	2017-03-01	Initial Version		
Steffen Fries	WG15	2017-05-30	Enhancement of OID, More details regarding the RADIUS profile. Clarification of relationship to PULL and PUSH models, which led to a re-write of the current describtion focussing solely on LDAP		
Steffen Fries	WG15	2017-07-28	Enhancement of the area of responsibility section. Standard of profile specific parameters in the access token.		
Frances Cleveland	Steffen Fries	2017-08-31	Editorial updates		2017-9-22
Steffen Fries	Frances Clevela nd	2017-09-22	Further Updates of the RADIUS profile with an index option to allow for multiple roles per user ith different AoR or Revision Deperecation of Profile C		
Steffen Fries		2017-11-22	Further description of Profile D and application itegration examples. Deletion of exisiting Profile C		
Steffen Fries		2018-02-22	Update on RADIUS, Inclusion of custom based role definition		
Steffen Fries		2018-04-30	Refinement of custom based role definition using XACML as proposed in IEC 62351-90-1		
Steffen Fries		2018-06-22	Aligned terminology of rights and permissions throughout the document, refinement of mandatory permissions, inclusion of JWT (based on the contribution of Arijit Bose) as Profile C. Introduction of security events (incidents and warnings) supporting IEC 62351-14.		
Martina Braun	Steffen Fries	2018-06-28	CD doc for circulation	CO	2018-06-28
Steffen Fries		2018-11-28	Incorporation of comment resolution (57/2056/CC) after WG15 meeting in 10/2018	WG15	2018-11-23
Steffen Fries		2018-01-17	Incorporation of final discussion of open issues after WG15 meeting in 01/2019	WG15	
Martina Braun	IEC	2019-05-17	Edited CDV to Project leader for next step	Steffen Fries	2019-05-20
Steffen Fries		2019-05-17	Incorporation of comment resolution for CDV after final discussion wuring web meeting in WG15 on July 1th, 2019 and discussion with IETF RADEST WG (alignment of port number assignment)	IEC	
Martina Braun	Steffen Fries	2019-08-16	FDIS document upload to IEC for circulation	IEC CO	2019-0-23

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE - DATA AND COMMUNICATIONS SECURITY –

Part 8: Role-based access control for power system management

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62351-8 has been prepared by IEC technical committee 57: Power systems management and associated information exchange.

The text of this standard is based on the following documents:

Enquiry draft	Report on voting
57/2180/FDIS	57/2197/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

This document includes code components i.e components that are intended to be directlyprocessed by a computer. Such content is any text found between the markers <CODE BEGINS> and <CODE ENDS>, or otherwise is clearly labeled in this standard as a code component.

The purchase of this document carries a copyright license for the purchaser to sell software containing code components from this document directly to end users and to end users via distributors, subject to IEC software licensing conditions, which can be found at: http://www.iec.ch/CCv1.

In the case of any discrepancy between the document and the code components, the code components take precedence.

In this document, the following print types are used:

Encoding in ASN.1 or XACML: `couriernew`

A list of all the parts in the IEC 62351 series, published under the general title *Power systems management and associated information exchange,* can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

This document provides a standard for access control in power systems. The power system environment supported by this document is enterprise-wide and extends beyond traditional borders to include external providers, suppliers, and other energy partners. Driving factors are the liberalization of the energy sector to include many more stakeholders, the increasingly decentralized generation of energy, and the need to control access to sensitive data of resources and stakeholders. This document supports a distributed security environment in which security is also a distributed service.

The power system sector is continually improving the delivery of energy by leveraging technical advances in computer-based applications. Utility operators, energy brokers and end-users are increasingly accessing multiple applications to deliver, transmit and consume energy in a personalized way. These disparate applications are naturally connected to a common network infrastructure that typically supports protection equipment, substation automation protocols, inter-station protocols, remote access and business-to-business services. Consequently, secure access to these distributed and often loosely coupled applications is even more important than access to an application running on a stand-alone device.

Secure access to computer-based applications involves authentication of the user to the application. After authentication, the types of interactions which that user can perform with the application is then determined. The use of local mechanisms for authorization creates a patchwork of approaches difficult to uniformly administer across the breadth of a power system enterprise. Each application decides with its own logic the authorization process. However, if applications can use a network to help manage access, a database can serve as a trusted source of user's group or role affiliation. Thus, the access to a shared user base can be controlled centrally. Each application can then examine the permissions listed for a subject and corresponding role and determine their level of authorization.

This document defines role-based access control (RBAC) for enterprise-wide use in power systems. It supports a distributed or service-oriented architecture where security is a distributed service and applications are consumers of distributed services.

In this document, the role of a user is transported in a container called an "access token" of that user to the object. Access tokens are created and administered by a (possibly federated) identity management tool. All access tokens have a lifetime and are subject to expiration. Prior to verification of the access token itself, the user transmitting the access token is authenticated by the object. The object trusts the management tool to issue access tokens with suitable lifetime. This enables local verification of the access token's validity at remote sites without the need to access a centralized repository (e.g. a centralized revocation list).

Four different access token formats are supported as four different profiles. Two of them are based on X.509 certificates and were already defined in IEC TS 62351-8. Two new profiles are defined as part of this document. The first new profile uses the JSON to encode the access token and the second new profile uses a vendor specific attribute in RADIUS to provide a migration option for environments already utilizing a RADIUS server to support access control. These access tokens may be bound to a specific transport or to a specific application. Common to all access token formats is the information contained, to allow a migration from one profile to another.

POWER SYSTEMS MANAGEMENT AND ASSOCIATED INFORMATION EXCHANGE - DATA AND COMMUNICATIONS SECURITY –

Part 8: Role-based access control for power system management

1 Scope

The scope of this part of IEC 62351 is to facilitate role-based access control (RBAC) for power system management. RBAC assigns human users, automated systems, and software applications (collectively called "subjects" in this document) to specified "roles", and restricts their access to only those resources, which the security policies identify as necessary for their roles.

As electric power systems become more automated and cyber security concerns become more prominent, it is becoming increasingly critical to ensure that access to data (read, write, control, etc.) is restricted. As in many aspects of security, RBAC is not just a technology; it is a way of running a business. RBAC is not a new concept; in fact, it is used by many operating systems to control access to system resources. Specifically, RBAC provides an alternative to the all-or-nothing super-user model in which all subjects have access to all data, including control commands.

RBAC is a primary method to meet the security principle of least privilege, which states that no subject should be authorized more permissions than necessary for performing that subject’s task. With RBAC, authorization is separated from authentication. RBAC enables an organization to subdivide super-user capabilities and package them into special user accounts termed roles for assignment to specific individuals according to their associated duties. This subdivision enables security policies to determine who or what systems are permitted access to which data in other systems. RBAC provides thus a means of reallocating system controls as defined by the organization policy. In particular, RBAC can protect sensitive system operations from inadvertent (or deliberate) actions by unauthorized users. Clearly RBAC is not confined to human users though; it applies equally well to automated systems and software applications, i.e., software parts operating independent of user interactions.

The following interactions are in scope:

– local (direct wired) access to the object by a human user, a local and automated computer agent, or a built-in HMI or panel;

– remote (via dial-up or wireless media) access to the object by a human user;

– remote (via dial-up or wireless media) access to the object by a remote automated computer agent, e.g. another object at another substation, a distributed energy resource at an end-user’s facility, or a control centre application.

While this document defines a set of mandatory roles to be supported, the exchange format for defined specific or custom roles is also in scope of this document.

Out of scope for this document are all topics which are not directly related to the definition of roles and access tokens for local and remote access, especially administrative or organizational tasks, such as:

– user names and password definitions/policies;

– management of keys and/or key exchange;

– engineering process of roles;

– assignment of roles;

– selection of trusted certificate authorities issuing credentials (access tokens);

– defining the tasks of a security officer;

– integrating local policies in RBAC;

NOTE Specifically, the management of certificates is addressed in IEC 62351-9.

Existing standards (see ANSI INCITS 359-2004, IEC 62443 (all parts), and IEEE 802.1X-2004) in process control industry and access control (RFC 2904 and RFC 2905) are not sufficient as none of them specify neither the exact role name and associated permissions nor the format of the access tokens nor the detailed mechanism by which access tokens are transferred to and authenticated by the target system – all this information is needed though for interoperability.

On the other hand, IEEE 1686 already defines a minimum number of roles to be supported as well as permissions, which are to be addressed by the roles. Note that IEEE 1686 is currently being revised.

Throughout the document security events are defined as warnings and alarms. These security events are intended to support the error handling and thus to increase system resilience. It is important implementations provide a mechanism for announcing security events.

Note that for the processing of security warnings and alarms resulting from security logging events and monitoring information there exists separate documents specifying the handling. More specifically, security event handling is specified in IEC 62351-14[1] while the handling of monitoring objects is specified by IEC 62351-7.

Note that warnings and alarms are used to indicate the severity of an event from a security point of view. The following notions are used:

– a warning is intended to raise awareness but to indicate that it may be safe to proceed;

– an alarm is an indication to not proceed.

In any case, it is expected that an operator's security policy determines the final handling based on the operational environment.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 61850-7-2, *Communication networks and systems for power utility automation – Part 7-2: Basic information and communication structure – Abstract communication service interface (ACSI)*

IEC TS 62351-2, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms*IEC 62351-3:2014, *Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP*
IEC 62351-3:2014/AMD2:2019[2]

IEC 62351-4, *Power systems management and associated information exchange – Data and communications security – Part 4: Profiles including MMS and derivatives*

[1] Under preparation. Stage at the time of publication: IEC/CD 62351-14:2019.

[2] Under preparation. Stage at the time of publication: IEC BPUB 62351-3/AMD2:2019.

IEC TS 62351-8:2011, *Power systems management and associated information exchange – Data and communications security – Part 8: Role-based access control*

RFC 2865, *Remote Authentication Dial In User Service (RADIUS)*

RFC 5246, *Transport Layer Security (TLS) Protocol version 1.2*

RFC 5288, *AES Galois Counter Mode (GCM) Cipher Suites for TLS)*

RFC 5289, *TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)*

RFC 5755, *An Internet Attribute Certificate Profile for Authorization*

RFC 5878, *Transport Layer Security (TLS) Authorization Extensions*

RFC 6749, *The OAuth 2.0 Authorization Framework*

RFC 7519, *JSON Web Token (JWT)*

XACML-RBAC, *XACML v3.0 Core and Hierarchical Role Based Access Control (RBAC) Profile Version 1.0, October 2014* [viewed 2019-11-15]. Available at: http://docs.oasis-open.org/xacml/3.0/xacml-3.0-rbac-v1-spec-en.html

3 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC TS 62351-2 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1
access token
evidence or testimonials concerning one's right to credit, confidence, or authority

3.2
area of responsibility
range of authority (for instance based on network segregation)

3.3
automated agent
computer program running on a single machine, which performs local and/or remote operations independent of user inputs

3.4
dynamic separation of duty
DSD
limitation of the availability of the permissions by placing constraints on the roles that can be activated within or across a user’s sessions

Note 1 to entry: DSD provides the capability to address potential conflict-of-interest issues at the time a user is assigned to a role. DSD allows a user to be authorized for roles that do not cause a conflict of interest when acted in independently, but which produce policy concerns when activated simultaneously. Although this separation of duty