10

EPHOS Security
Procurement of secure open systems

N. H. Pope and J. G. Ross
Security & Standards Consultancy Ltd.
Suite A, 192, Moulsham Street, Chelmsford, Essex, CM2 0LG
United Kingdom
Phone: + 44 1245 495018 Fax: +44 1245 494517
E-mail: POPE@SECSTAN.DEMON.CO.UK:
ROSSJG@ATTMAIL.COM

Abstract

This paper outlines the approach taken in the security module of the European Handbook for Procurement of Open Systems (EPHOS). EPHOS is a European Commission led development of a suite of handbooks for the procurement of open system services such as data communications, messaging, directories, EDI and operating systems. The paper describes a Basic Security Scenario which is used as the baseline for the security provisions defined in the EPHOS security module. The paper describes two ways that procurers may use EPHOS security. One provides a default set of options in a "Procurement Profile" which matches common business security concerns. The other route provides a set of decisions for selecting "Procurement Clauses" for options best fitting the procurement situation. The paper outlines the default options selected for the X.25, X.400 and EDI "Procurement Profiles" as well as the generic security techniques which are used in support of the range of application areas. The paper describes the on-going work to address requirements for security of other application areas and concludes by identifying the unique features of EPHOS security.

Keywords

Security, open systems, baseline security policy, message handling systems, data communications, procurement

1 INTRODUCTION

The general aim of EPHOS (the European Procurement Handbook for Open Systems) is to provide straight-forward guidance for procurers to specify requirements in procurement documents for information systems. Any choices are described in business terms so that they can be easily understood by a procurer who is not a specialist in the technology involved. As

S. K. Katsikas et al. (eds.), *Information Systems Security*

much as possible the choices are reduced to a few basic approaches to address the most common requirements using solutions that are generally available in the computer market. The EPHOS handbook only uses those technical terms and concepts which are absolutely necessary for selecting the appropriate procurement choices and explains these terms using language which the procurer can easily relate to his general business concerns.

Security has been recognised as an important factor in the procurement of computer systems and, although security is generally procured as an adjunct to a communication, system platform or application services, it is addressed in a own part of the EPHOS handbook. The authors of this paper, assisted by other specialists in particular aspects of security, were given the task of producing the EPHOS security "module" as part of the European Commission EPHOS project. The EPHOS security module had to fit in with the general approach of EPHOS, providing clear and simple guidance for choosing the appropriate security solutions. EPHOS security was required to provide definitive statements that could be incorporated in a statement of requirement by a procurer who has little, if any, specialist knowledge in security.

The security module addresses the requirements of the most common business environments. It is the objective to meet the most prevalent risks that occur in such environments. Environments with a high security risk (e.g. banking, military operational systems) are not of prime concern.

The other modules of EPHOS, to which security could be applied, covers a range of communication, application services. The initial version of the general EPHOS guide (EPHOS 1) addressed data communications based on the X.25, messaging based on X.400 and file transfer access and management. The next versions (EPHOS 2 and 2bis) added a number of other services including operating systems, database access, Electronic Data Interchange, virtual terminal, directory services, OSI management. Security was included as part of the EPHOS 2bis.

The first version of the EPHOS (2bis) security module specifically addresses security of X.25 data communications, X.400 messaging and Electronic Data Interchange whilst providing a general framework for security in other topic areas. Specific advice for other areas is to be developed in the next phase of EPHOS (2c).

2 BASELINE SCENARIO

For EPHOS security to meet its objectives and provide straightforward guidance without a proliferation of choices, it was necessary to identify the most prevalent security concerns of business environments.

Traditionally, the application of security has been based on an analysis of the risks associated with a particular computing environment. The selection of security provisions is based upon an analysis of the costs of providing security weighed against the potential for losses due to security threats against the computer systems. The choices are made on a case by case basis to achieve the most cost effective solution.

Initially it was proposed in EPHOS security to identify the range of security solutions that were available and guide the procurer in selecting the most appropriate solution based on specific security concerns identified for the procurement. This lead to large and complex decision trees with a range of technical solutions which could be brought together in a

number of different ways. This was found to be too complex for the target audience of procurers not specialised in security.

Thus, whilst it was agreed that the procurer should be encouraged to analyse his specific security risks, it was recognised that assumptions would need to be made about the risk environment for the procurement. This could then be used as the basis for the security functionality necessary for EPHOS procurements.

In a number of European countries there already exists guides and baselines for general commercial security. In the UK there is a British Standard: Code of Practice for Information Security Management (BS 7799), and in Germany there is an IT (Information Technology) Baseline Protection Manual. These provide a useful general guide to the security of IT systems. However, they are primarily aimed at guidance on procedures and practices for security. They do not identify specific IT procurement requirements for the procurement of IT systems, rather they describe general procedures for using security functions that commonly exist in the IT environment.

Therefore, a security scenario was developed for EPHOS security which identified a set of basic assumptions about the environment in which EPHOS procurements occurred. This "basic security scenario" was then used as the basis for selecting the choices for security functionality to be included in EPHOS. This security scenario took into account the security concerns inferred from the European codes of practice and baselines. In developing the baseline the technical development team considered a range of procurement situations covering office automation, EDI trading and information distribution systems. Also, they took into account existing EPHOS procurement scenarios identified in the general guide produced for the EPHOS technical development teams .

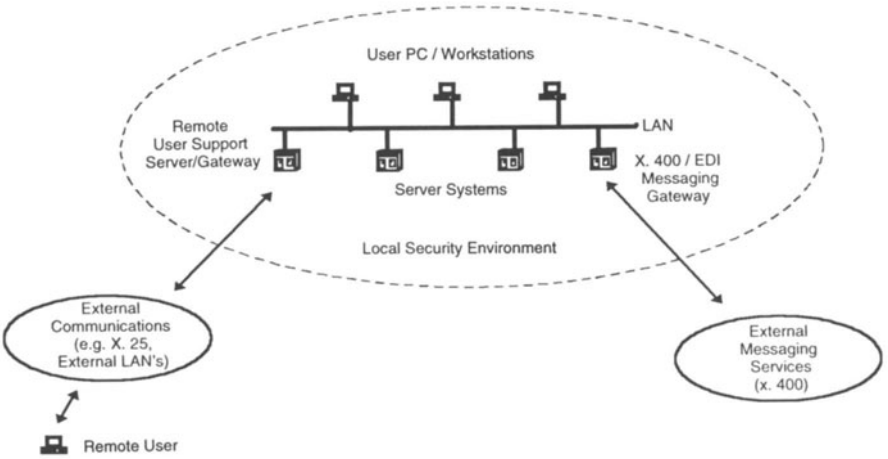
The EPHOS "basic security scenario" assumes that the computing services being procured are to be placed in a building or site which is physically secured. Direct access to the computing facilities is assumed to be restricted to a known community of users. It is assumed that the building or site, and the computer systems it contains, already had some security controls in place which were applied by an administration with a single authority having overall responsibility for security. The collection of computing facilities held in the physically secured site or building is termed the "local security environment".

A second assumption of the "basic security scenario" is that communication and messaging services in and out of the local security environment are routed through a special purpose gateway / firewall computer system which controls external access. Only authorised users are allowed from the external communications environment into the local security environment.

These two assumptions enable the EPHOS security module to concentrate on the threats to the external communications and messaging services.

An example of this security scenario is illustrated in the figure shown below.

This example illustrates several personal computers and workstations linked via a local area network held in a building or site which has restricted access. External messaging services are supported via a special purpose message gateway. Other services are provided on a special purpose support system which is designated for external access and restricts onward access into the local environment. Security measures are to be in place within the local security environment, whereas the external data communications and messaging services are open to attack.



The EPHOS Security module initially concentrates on addressing the threats to the external X.25 communication services as well as X.400 and EDI messaging services. Whilst security risks to the local environment can be significant, the assumption of this scenario is that the appropriate local security measures are in place (for example appropriate local authentication, access control measures are in place).

The security measures taken for X.25 communications and X.400 messaging can also to used to indirectly protect other application and data services from external threats. For example, when using the File Transfer and Management standard protocol to remotely access files security of the lower layer data communications can protect the integrity and confidentiality of the file during transfer. Similarly, a formatted document can be carried in a protected X.400 message to counter attacks when carried in the messaging environment.

3 PROCUREMENT ROUTES THROUGH EPHOS SECURITY

The EPHOS Security module offers two routes for selecting the appropriate requirement statements for their call for tenders.

The first path is for use by procurers who are not aware of any specific security requirements by wishes to provide a baseline for security. For this path the EPHOS security module provides an "EPHOS Procurement Profile" which selects a default set of options for the procurer. The procurer can refer to the EPHOS Procurement Profile in call for tenders to imply a set of profiles and options which support baseline security services (for example: access control, authentication and integrity). In some cases the EPHOS procurement Profile includes optional extra security services which the procurer may select to meet additional security requirements (for example: confidentiality and non-repudiation).

The second path is for use by procurers who wishes to tailor the security provisions to his particular security requirements. For this path the EPHOS security module provides "EPHOS Procurement Clauses" which specify requirements for particular options. The procurer is guided in selecting the options and associated Procurement Clauses which meets his particular

needs using a decision tree. The procurer can copy the appropriate EPHOS Procurement Clauses into his call for tender.

The selection of an EPHOS Procurement Profile implies a default set of EPHOS Procurement Clauses.

The EPHOS security module defines Procurement Profiles and Procurement Clauses for security of:

- Data communications using permanent access to an X.25 network;
- Message Handling Systems based on X.400;
- EDI carried over messages handling systems based on X.435;
- EDI encoded using the EDIFACT syntax

For security of general OSI data communications the EPHOS security module defines additional Procurement Clauses which are not included in any EPHOS Procurement Profile. This is because the approach uses security protocols for which, at the time the EPHOS text was initially prepared, no standardised profiles existed.

The EPHOS Procurement Profiles and Procurement Clauses for security go much further in identifying requirements on the supplier than existing profiles (such as defined by EWOS for Europe, OIW for America and by ISO in international standardised profiles). The EPHOS security module also includes requirements for the use of generic security techniques such as assurance, audit, cryptographic algorithms and key management. These requirements are generally common to a range of application area and so are addressed in a general section of the EPHOS security module.

4 PROTECTION OF OSI AND X.25 COMMUNICATIONS

Two basic security concerns were identified for the security of OSI (Open Systems Interconnection) including X.25 data communications. Firstly, there is a common concern that computer systems placed on a public X.25 network are not made generally accessible to anyone on the public network. This provides a first line of defence reducing the community where potential threats may occur down to a identifiable group. The X.25 standard includes facilities to support restriction of access through X.25 networks called "Closed User Groups".

The use of X.25 Closed User Groups depends on the network provider enforcing the closed user groups and ensuring that data connections are routed correctly. If the management of the public network is subverted then Closed User Group security no longer protects the user system from attack. Furthermore, X.25 Closed User Groups do not protect the integrity and confidentiality of the data communications (i.e. no protection is provided against data being modified during transfer or information being revealed to third parties as it passes through the communication links and packet switches).

A second choice for secure OSI and X.25 communications using cryptographic protection is included in EPHOS to provide a higher degree of security. This approach can be used if the network provider cannot guarantee to enforce the required security (correctly route addresses and integrity and confidentiality). Two standards have been recently developed which can provide the appropriate protection: the Network Layer Security Protocol (ITU-T Rec. X.273 | ISO/IEC 11586) and the Transport Layer Security Protocol (ITU-T Rec. X.274 | ISO/IEC

10736). The standards are independent of the sub-network and can be used for any OSI based communications network.

The specification of technical choices in EPHOS is generally specified around International (or European) Standardised profiles. For X.25 communications the profile recommended by EPHOS is defined in ISO ISP 10609. This profile, however, does not cover use of X.25 Closed User Groups and, at the time when the scope of EPHOS security was agreed, did not include use of the Network or Transport Layer Security Protocols.

In the case of X.25 Closed User Groups reference is made to the optional user facilities in the X.25 base standard (optional X.25 user facility P14.1) as the default for the EPHOS Procurement Profile. Further requirements are also placed on the network provider to ensure the correctness of routing.

In the case of security using cryptographic protection, no EPHOS Procurement Profile is identified. Procurement clauses are provided which reference either the Transport or the Network Layer Security Protocols. A decision tree is provided to identify when one or other of the security protocols is more appropriate. As no profiles existed the selection of specific options within the protocols is left to the supplier. Also, as very few products are available based on these standards the supplier is also allowed to offer solutions based on cryptographic techniques which provide the same security services. With the emergence of profiles for the Network Layer Security Protocol (pDISP 10608 parts 7 and 8, pDISP 10609 parts 16 and 17, pDISP 10613 parts 19 and 20), it is hoped that future enhancements to EPHOS security will make reference to the appropriate profiles in an EPHOS Procurement Profile.

5 PROTECTION OF X.400 MESSAGING

The main requirement identified in the security scenario is to protect messages passing in and out of the local security environment up to a remote user's messaging system. The primary concern is considered to be protection against masquerade and data modification, thereby countering attacks from bogus messages. In some cases it is considered necessary to be able to ensure the confidentiality of messages. Also, as the messaging system might be used to support the exchange of legally binding information, the need for optional non-repudiation services was also identified. It is considered that the message may pass through a number of public message systems and so it would be difficult to obtain any assurance that all the potential paths for the messages could be trusted unless the messages themselves are protected.

Thus, for EPHOS the security of X.400 messaging is based around the "S0" security profile as defined in ISO/IEC ISP 10611 was selected. S0 provides end to end (user agent to user agent) security protecting the message across the messaging environment without the need to secure any of the message switches (called message transfer agents in X.400). S0 uses digital signature mechanisms to provide authentication and integrity of messages. The signature is added to the message by the originator and validated by the recipient. This signature can also be validated as it passes though the messaging gateway.

The X.400 messaging security profile also includes an optional variant of the S0 profile which includes security (called "S0C"). The selection of S0C is identified as an alternative choice for environments where confidentiality is of concern.

Non-repudiation is commonly achieved through use of appropriate operating procedures for the management of keys and the use of trusted third parties. Thus, for procurement requiring

non-repudiation with X.400, EPHOS identifies additional constraints on the operating procedures and use of trusted third parties to provide non-repudiation.

Other options (called "S1" and "S2") also exist in the standard profile. These options include additional services which can provide some hop by hop protection and enable the flow of messages between message switches to be controlled. Whilst these were initially considered as choices within EPHOS security it was decided to rule out these options as were not seen as essential for countering the risks identified for the basic security scenario.

6 PROTECTION OF EDI MESSAGES

The requirements for protection of EDI are broadly similar to those required for general X.400 messaging services. Again, the authenticity and integrity of messages was identified as being of prime concern. As EDI is concerned with commercial transaction there is also a need for some form of non-repudiation or proof of origin, and in some cases also receipt. Confidentiality was also identified as a potential concern for some environments.

Two possible approaches to the security of EDI are addressed in EPHOS security. One is to use the facilities of X.400 messaging security applied to the X.400 EDI content (X.435), the other is to apply security as part of the EDI message syntax (i.e. EDIFACT security). The first is most appropriate to procurements incorporating X.400 and enables the similar protection to be applied to inter-personal messages as well as EDI messages. The use of EDIFACT security enables the protection to be applied across other type of messaging environment (e.g. Value Added Data Services). Also, with EDIFACT security the protection can be applied to individual parts of the EDI interchange (e.g. individual orders or invoices).

EDI security using X.400 is based on the S0 or S0C profiles, as recommended for general X.400 security, extended for EDI. The X.400 security extensions for EDI are defined in the international profile ISO/IEC ISP 12063. This profile can either be used to provide "proof of origin and receipt" or full non-repudiation. EPHOS security defaults to proof of origin and receipt unless specific non-repudiation requirements are identified.

EDI security using the EDIFACT syntax is based on the use of the EDIFACT security implementation guidelines and recommendations for UN/EDIFACT message level security. The options in this recommendation for authentication and non-repudiation of sender are mandated with choices for non-repudiation of receipt and confidentiality.

7 GENERIC SECURITY TECHNIQUES

There are a number of aspects of security (e.g. assurance, algorithms, security management), not directly addressed by the standard profiles described above, which need to be specified in a procurement. Generally, these techniques are common to a range of security profiles and so in EPHOS security, requirements on these techniques are specified in a common section which is referenced, as appropriate, in support of specific EPHOS Procurement Profiles.

7.1 Assurance

This was an area where there was conflict between the desire to achieve a level of security which best matched the concerns of the environment, and the aim of EPHOS to provide simple guidance based on the minimum necessary choices. It was not possible to require a

specific level of assurance as, given the potential cost penalty of high assurance products and the variability of such costs depending on the maturity of the market. It is only possible to make such choices given information of what the market has to offer at a specific time and what the procurer is prepared to spend on security. Thus the resulting "procurement clause" gives maximum flexibility, allowing the supplier to offer the highest level assurance he could provide for what he considers to be the best value for money. Preference is given to the ITSEC criteria, or the American or other international equivalents, but suppliers are given the option to offer "self certified" products.

7.2 Audit Logging and Security Management

It is recognised that the provision of audit logs are important for monitoring the security aspects of the computer system as well as providing a tool for analysing any possible security violations. Thus it was considered necessary in EPHOS security to place general requirements on systems to support the collection of audit information. Whilst there exists standards for collection of audit information (e.g. the OSI systems management audit function), which are covered in the EPHOS network management module, these requirements were independent of whether this is made available remotely through standard protocols.

Similarly, general requirements were identified for the provision of facilities to manage the security services and mechanisms.

7.3 Cryptographic Techniques, Algorithms and Key Management

Cryptographic techniques are used in the security of a number of the communication and application services covered by EPHOS. These security protocols and their profiles generally do not specify the use of any particular cryptographic algorithms. Nor are there any algorithms which are generally recognised for business use across Europe. The EPHOS security technical team recognised the need to establish common algorithms if interoperability is to be achieved between different equipment. However, in the absence of any agreed approach, the EPHOS security module generally leaves the selection of the algorithms to the manufacturer. It is required that any manufacturer specific algorithms are either approved for use by the national authority or other authority establish by the user community, or registered in the international register for cryptographic algorithms established under ISO/IEC 9979.

Similarly, whilst there exists a framework for certain aspects of the management of asymmetric keys (sometimes called public keys) in the CCITT Rec. X.509, the supplier is generally left to select the approach for most aspects of key management.

As identified earlier in the discussion on X.400 messaging security, additional requirements are identified for procurements providing non-repudiation with digital signatures.

8 FUTURE DIRECTIONS

The current version of EPHOS security module only specifically addresses security of X.25 communications, X.400 messaging services and EDI.

Work has started on the development of an enhanced version of the EPHOS security module. Whilst the scope of this activity has yet to be agreed, it is the initial objective to cover security for a range of topics including:

- Document Formats,
- File Transfer Access and Management,
- Distributed Transaction Processing,
- OSI Management,
- Metropolitan Area Networks (MAN),
- Local Area Networks (LAN),
- Operating Systems
- Data Base Enquiry
- Directory Services
- LAN/WAN Interworking
- Virtual Terminal
- TCP/IP & OSI coexistence

Special attention will be given to requirements for secure gatewaying. This will concentrate on those services which need to cross from the external to the local security environment (e.g. directories, LAN/WAN interworking, virtual terminal and linked LANs and interworking with TCP/IP). Whilst no standards exits in this area, this technique has recently become common practice. Generally, such devices control access between private networks and open networks such as the Internet.

9 CONCLUSIONS

EPHOS security is unique in the guidance it provides for procurement of security related facilities. It defines default solutions which a procurer can directly adopt without concerning himself with the details of security. It also provides an alternative approach which enables the procurer to select options meeting his own specific security concerns.. The guidance is given in clear terms for the non-security specialist whilst being precise enough to identify detailed technical requirements to suppliers.

EPHOS security goes further than existing profiles (as defined by standardisation bodies such as EWOS, OIW and ISO). It covers requirements for aspects of security, not conventionally covered by such existing profiles, which are needed in a complete procurement specification (e.g. assurance, security management, selection of algorithms and key management).

The basic security scenario provides a common reference for identifying the risks across the range of EPHOS topic areas. By adoption this common scenario a more cohesive approach to security in EPHOS has been achieved.

In developing the EPHOS security module the importance of isolating local threats from external threats was identified. This requires the use of secure gateways or firewalls to reduce the risks of external threats on local computing facilities. Procurement of such devices is aimed to be addressed by the next version of EPHOS security (2c).

The adoption of a common approach to security, such as EPHOS is hindered by the lack of agreement on cryptographic algorithms. Without a common agreement of algorithms for use

across Europe, the aim of EPHOS to provide a common basis for procurement cannot be achieved. This is aggravated by the lack of commonly accepted solutions for key management covering the lifetime of the key from creation through distribution and use onto revocation and final destruction. This needs to address the management of symmetric keys as well as asymmetric keys.

The development of EPHOS security met many difficulties in trying to satisfy a range requirements: to be precise enough for suppliers to use, simple enough for non-specialist procurers to use and not leave the procured system open to major risks. Also, in many cases there were no existing standardised solutions for security which EPHOS security could use. Despite these difficulties it is considered that the EPHOS security module provides a clear and precise tool for procurement of secured products.

Because of its unique features it is considered that EPHOS security could have a significant impact on the future of the IT security market.

10 ACKNOWLEDGEMENTS

The author's wishes to acknowledge the contributions made by Robin Sherman and Roy Jones in the development of the EPHOS security module, and by the members of the EPHOS Public Procurement Group, particularly Jim Bond (CCTA, UK), Peter Shuttleworth (MoD, UK), Hans Daniel (BSI, Germany) and Steve Mathews (PC Security, EWOS) as well as the co-ordinating editor responsible for EPHOS security, Per Knutsen (Fischer & Lorenz) in helping to make the EPHOS Security module a clear and well structured document.

11 REFERENCES

BS 7799 British Standard: Code of practice for Information Security Management

IT Baseline Protection Manual - German Information Security Agency

CCITT Recommendation X.25 (1993), Interface between Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE) for terminals operating in Packet Mode and connected to public data networks by dedicated circuits.

ISO/IEC ISP 10609: 1992 Information Technology - International Profiles TB, TC TD and TE - Connection mode Transport Service over connection mode Network Service

ITU-T Recommendation X.273 (1994) | ISO/IEC 11577 (1995) Information Technology – Open Systems Interconnection – Network Layer Security Protocol

ITU-T Recommendation X.274 (1994) | ISO/IEC 10736 (1995) Information Technology – Open Systems Interconnection – Transport Layer Security Protocol

ISO/IEC PDISP 10608-7 Security employing the Network Layer Security Protocol - Connectionless mode, for TAnnn profiles

ISO/IEC PDISP 10608-8 Security employing the Network Layer Security Protocol - Connection-mode with SDT-PDU based Protection over X.25 packet switched data networks using virtual calls, for TA1111 / TA1121 profiles

ISO/IEC PDISP 10609-16 Security employing the Network Layer Security Protocol - Connection-mode with No-header, for TB/TC/TD/TE nnn profiles

ISO/IEC PDISP 10609-17 Security employing the Network Layer Security Protocol - Connection-mode with SDT-PDU based Protection for TB/TC/TD/TE nnn profiles

ISO/IEC PDISP 10613-19 Security employing the Network Layer Security Protocol - Connectionless mode, for RAnnn profiles

ISO/IEC PDISP 10613-20 Security employing the Network Layer Security Protocol - Connection-mode with SDT-PDU based Protection over X.25 packet switched data networks using virtual calls, for RA1111 / RA1121 profiles

ITU-T Recommendation X.400 (1992) Message Handling Systems (equivalent to ISO/IEC 10121 (1990) – Message-Oriented Text Interchange Systems (MOTIS) with corrigenda)

ITU-T Recommendation X.435 (1992) Message Handling Systems - Electronic Data Interchange Messaging System (equivalent to ISO/IEC 10121-9)

ISO/IEC ISP 10611: 1994, Information technology - International Standardized Profiles - Message Handling Systems - Common Messaging

ISO/IEC ISP 12063: 1994 Information technology - International Standardized Profiles - Message Handling Systems - Electronic Data Interchange Messaging

BIOGRAPHIES

Nick Pope is an associate consultant of Security & Standards Consultancy Ltd, and a member of the EPHOS Security technical drafting team. He has made major contributions to European and International standards for security of communications and distributed applications. He has had over twenty years experience in computer and communication systems and has provided consultancy services to UK and European government departments including the Ministry of Defence, Dept. of Trade and Industry as well as several international computer companies.

John Ross is a Director of Security & Standards Consultancy Ltd. John has over 25 years experience in Information Technology, he has made major contributions to the development of IT security and standards both Internationally and in Europe. He leads the EPHOS technical Drafting Team on EPHOS security. John has provided Consultancy services to major UK government departments, including; the Cabinet Office, Ministry of Defence, Home office as well as international organisations and companies, such as NATO and SWIFT.