

Prepaid Voucher Vendor Security Manual

// Præsidium has produced a Best Practice Manual ... specifying the nature and type of security requirements and standards needed for the secure production of prepaid vouchers. //

How secure is your Prepaid Voucher producer?

The biggest growth service in the mobile world over the last few years has been Prepaid – the risk to a telecom operator is very dependent on the integrity of the vendor's product (vouchers) and the security and quality arrangements surrounding production. As mobile operators worldwide are heavily reliant on revenues from their prepaid service, the security of the voucher is increasingly becoming more important as it is still the main method of topping up airtime, especially in cash driven societies.

Having completed vendor security reviews at over 20 manufacturing facilities globally, Præsidium has seen the different standards and levels of protection being afforded to the production of prepaid airtime vouchers (in effect hard currency).

Operators and vendors alike have commissioned Præsidium to evaluate the physical vouchers. This has revealed a number of different production techniques being used which underpin the fundamental principles of the product's security. What is finally being delivered to the end user must be secure, but as with all commercially sensitive products, security comes at a price. Præsidium has found that some operators are primarily concerned only with the cost of voucher production and that security is secondary, if considered at all.

However, there are a number of operators that have commenced a program of vendor auditing that incorporates a team approach consisting of security and quality personnel who perform audits of the production facilities. Some operators have a number of companies producing vouchers for their prepaid service. To ensure the integrity and quality of the product being provided, operators conduct security audits and in doing so are now seeing the benefits of introducing a uniformed approach to vendor security auditing. This aspect of risk management is still relatively new to most operators and external guidance and support is initially required.

Contact Details:

Præsidium Services Limited
Atlantic House
Imperial Way
Reading
RG2 0TD
United Kingdom

Phone: +44 118 922 4444

Fax: +44 118 922 4432

admin@praesidium.com
www.praesidium.com

praesidium

Præsidium's approach to Vendor Auditing

Detailed below is an introductory guide to the areas to be incorporated by the operator's Auditing Team.



To support these initiatives and based on Præsidium's professional experiences, Præsidium has produced a Best Practice Manual to provide both telecom operators and prepaid voucher manufacturers with a document specifying the nature and type of security requirements and standards needed for the secure production of prepaid vouchers. Præsidium has attempted to ensure that explanations within the Manual are detailed enough for someone who has never visited a production facility to be able to follow and understand. The contents page summary is included at the end of this article for reference purposes.

“ There are no internationally recognised standards in place for the production of prepaid vouchers. ”

Præsidium appreciates that there are voucher manufacturers ranging from internationally recognised companies supplying a global market to small private businesses servicing the local telecom market. However, there are no internationally recognised standards in place for the production of prepaid vouchers as there are for other financial products, such as credit cards or SIM card production, (GSM Association Security Accreditation Scheme). The Manual addresses this position and has been produced to benefit both the operator and vendor.

The different operational standards that exist are influenced by the size of the business, technology deployed and supporting business processes, procedures and personnel employed. These differ from vendor to vendor but Præsidium's Manual has been produced by adopting a level perspective that can be used to establish a secure operating environment irrespective of the size of the business. The Manual determines the criteria that vendors should be required to meet and maintain to be a preferred supplier to an operator.

From the vendor's perspective, they should ensure that as part of their sales initiative they are offering a secure product to the operator and ultimately the end user – the customer. Vendors are therefore realising

that by setting and following certain standards of security they are able to increase their sales quotas as operators have more confidence in the products being provided.

The Manual has two main purposes from an operator's perspective. Firstly, to determine the standard of processes, procedures and overall security requirements it demands and will impose on vendors in order for them to be considered as secure manufacturers of their product. To achieve this, the operator can provide the vendor with appropriate sections of the Manual with a requirement for conformance within a defined period of time, which will then be subsequently audited during the contractual lifetime. Secondly, the Manual provides the operator's Auditing Team with practical guidelines that would be used during vendor audits to ensure compliance with security standards set and enables the auditors to report back to the operator's management.

// The final product is what needs to be secured so that it protects the financial value of the operator. //

From a vendor's perspective, the Manual has been developed to provide them with a comprehensive understanding of the security standards, processes, procedures and personnel requirements that must be in place throughout all areas of a voucher production facility. This will enable vendors to meet with the expectations of the operator and can be used by new entrants to the market as a guide to what is expected. For the more established vendors, it can be used to benchmark their current security strategy and ensure that they are setting and adhering to the required standards.

However, it must be remembered that the most secure production facility will not necessarily result in an overall secure product being produced. The final product is what needs to be secured so that it protects the financial value of the operator. Additionally, if the operator's own internal procedures and security initiatives are not fully controlled with appropriate security measures implemented, then the risk exposure to fraud will still remain high.

For ease of reference within the Manual, areas that the vendor should primarily comply with have been included within a boxed area with narrative at the start of each section where appropriate. This narrative also incorporates the actions required by the operator's Auditors. Præsidium has avoided using any grading categorisation against the areas contained within the Manual due to the generic nature of the requirements of different operators. The respective vendor and operator's Audit Team will be able to classify requirements by, for example, Critical/Necessary/Desirable upon reviewing the Manual and assessing the requirements against local practices and circumstances.

The security-auditing program is an evolving process and operators are best placed to determine the use of the Manual and how their specific vendors will ultimately be required to comply. The vendor will be able to use the Manual to sell security to existing and prospective clients who are looking for an assurance that the vendor is able to securely produce their specific prepaid product.

Should any operator or vendor require additional support from Præsidium, this can be discussed by contacting us.

Præsidium is an industry leading independent Communications Risk Management Consultancy, which specialises in Revenue Assurance, Fraud Management, Network Security and Business Continuity across the wireless, wireline and internet industries. Over the last decade, Præsidium has conducted consultancy assignments for more than 100 telecom operators worldwide and for a wide range of OSS vendors.

For further information, please contact us.

Manual Contents Page

1 Purpose

2 Introduction

2.2 Security Auditing Stages

2.2.1 Stage 1 – Internal and External Security Provisions

2.2.2 Stage 2 - Production and Personalisation Area

2.2.3 Stage 3 – Data Management

2.2.4 Stage 4 – Artwork and Raw Materials

2.2.5 Stage 5 – Packaging

2.2.6 Stage 6 - Product Movement, Storage and Distribution

2.2.7 Stage 7 - Additional Considerations

3 Policies and Procedures

4 Transfer and Receipt of Data

5 Personnel

6 Security Zone Classification

7 External Physical Security

8 Internal Physical Security

9 Storage of Raw Materials

10 Voucher Body Cutting

11 Artwork

12 Production/Personalisation Area

13 Packaging Area Environment

14 Storage

15 Distribution and Logistics

16 Movement of Vouchers Between Areas

17 Business Continuity and Disaster Recovery Planning

18 Health and Safety

19 Auditing

20 Third Party Vendors

21 Product Risk Analysis and Voucher Integrity Testing

22 Contractual Clauses for Consideration

23 Continuous Improvement

The full contents pages can be supplied by Præsidium if requested.