PSA
Phone-paid Services Authority

Code 15 Guidance note – Systems Standard

All systems, including payment and consent verification platforms, used for the provision of and exit from phone-paid services must be technically robust and secure.

This guidance note sets out the PSA's expectations and provides more detail on how phone-paid service providers (network operators, intermediary providers and merchant providers) can comply with the Systems Standard and Requirements. To support compliance with the Systems Standard, this guidance provides more detail on:

- technical expectations
- risk management and control
- staff roles and responsibilities.

All platform providers must take reasonable actions within the context of their role to ensure that all of the phone-paid services they are involved in are of an adequate technical quality, including the mechanisms used to deliver services to and to enable exit of services by consumers.

If you have any queries about the guidance set out in this note or want to discuss your approach to compliance with the Systems Standard, please email us at compliance@psauthority.org.uk.

Expectations around robust systems

Robust systems are those which have adequate technical and risk control procedures and records that demonstrate any charging cannot have been initiated in any way other than from the informed consent of a consumer.

Systems expectations can be split into three categories:

- technical expectations
- risk management and control
- staff roles and responsibilities.

These expectations apply to all platforms. This includes payment/consent platforms provided by any intermediary provider who is part of a value chain, and consent verification platforms provided by third parties (whether they sit within a value chain, or have been contracted by a merchant provider, intermediary provider, or network within it, or indirectly provide consent verification services to it).

Technical expectations
These are set out at Annex 3 of the Code. The PSA's technical expectations for payment and consent verification platforms take into account that it is possible to arrive at robust proof of informed consent through different approaches depending on the design of a platform's technical architecture. Nonetheless, there are universally accepted standards regarding the underlying software platforms used to operate, and the protocols they use to interface with web pages and other external systems. The technical expectations which we set focus on these universal standards.

Risk management and control
Poor risk management can lead to Systems being compromised. It is important that all relevant providers involved have adequate processes to quickly identify, record, communicate and control risk, and to incorporate lessons learned into processes.

All parties involved in provision of phone-paid services should maintain a security risk/issues register. The register should record any identified risks or issues on an ongoing basis, and set out as a minimum the following:

- an explanation of the risk or issue – in the case of an issue, the explanation should also set out exactly when and how it was discovered, and by whom
- the actions taken to mitigate/resolve the risk/issue – with a timestamped record of who has signed them off as being complete and when
- any further ongoing actions (which can be transferred to "actions taken" as above, once they are complete and signed off)
- the individuals within the organisation responsible for ongoing actions.

The PSA also recommends that active threat monitoring measures are implemented to monitor systems and alert staff in real time. These measures should aggregate data from across the platform, understand traffic patterns, and provide detailed information about potential attacks or exploits. This should include, but not be limited to:

- leveraging threat intelligence from previously seen attacks
- analysing consumer behaviour – e.g. transaction logs, transaction times, user agent/device, x-header requests, associated URLs, IP addresses, time deltas between double opt-ins, repeat transactions, unfinished transactions, repeat unfinished transactions and their frequency
- analysing merchant provider behaviour – e.g. what kind of data they access and how frequently, whether apps are requesting payment pages
- performing "attacker behaviour" analytics
- setting intruder traps – e.g. decoy network services or credentials
- conducting proactive threat hunts

- conducting “red team/blue team” penetration testing using discovered malware.

All parties involved in the provision of phone-paid services should act on any security alerts or flags, whether from their own monitoring or information shared by others, in a timely manner (Code Requirement 3.10.5). An example template for recording security breaches, or attempted breaches, is attached at Appendix B. The use of this template is voluntary; however, it does set out the level of detail the PSA would expect to receive around any security breaches or attempted breaches where relevant to an investigation.

The PSA recommends that each platform should be tested by a CREST-accredited third party or a third party with an equivalent accreditation on an annual basis. Testing should identify and score exploits according to the OWASP taxonomy and the CVSS scale. The results of these tests should be made available to all mobile network operators and provided to the PSA on request. Any identified exploit with a CVSS score of 4.0 or over should be fixed or mitigated immediately. The platform, and services that are using it (or in the case of third-party consent verification platforms, just the services that are using them) may be in breach of the relevant Code Requirements (Code Requirements 3.10.4, 3.10.5 and 3.10.6) until the fix has been completed, as independently verified by the tester.

In line with DDRAC Requirements, intermediary providers should have contracts in place which allow them to suspend or terminate payment their contractual relationship with any merchant or third-party consent verification platforms on the basis of non-compliant activity, such as charging consumers without informed and robust consent, or where they reasonably suspect that such activity has or is occurring.

Also in line with DDRAC Requirements, mobile network operators should have contracts in place which allow them to suspend or terminate their contractual relationship with providers in circumstances where non-compliant activity is discovered. In addition, they should take effective action against intermediary providers whose platforms facilitate non-compliant activity, such as charging consumers without consent or where they reasonably suspect this to be the case.

This should include clear, documented consideration of whether intermediary providers should be suspended or have their contracts terminated in relation to more serious incidents and clearly documented consideration of whether a sequence of incidents warrants suspension or contract termination.

The PSA recommends that mobile network operators should have contracts in place which permit them to conduct further random testing by the accredited third party at any time on any intermediary provider’s payment platform (Code requirement 3.10.12), and to document any findings and when and how improvements are made as a result of them.

The PSA’s Guidance on DDRAC provides further guidance on the PSA’s expectations in respect of risk management and control.

Network operators and intermediary providers must implement a **coordinated vulnerability disclosure scheme** (Code Requirement 3.10.13**)**. This will enable providers to work cooperatively with security researchers and other relevant persons to find solutions to remove or reduce any risks associated with an identified vulnerability in their services and/or systems. The aims of a vulnerability disclosure scheme include ensuring that identified vulnerabilities are addressed in a timely manner; removing or minimising any risks from any identified vulnerabilities; and providing users with sufficient information to evaluate any risks arising from vulnerabilities to their systems.

There are a range of resources available to providers to assist them in developing coordinated vulnerability disclosure schemes including an ISO standard.

Staff roles and responsibilities

To enable the identification of risks and ensure they are communicated and controlled, the PSA has set out expectations around roles and responsibilities and staff training. Staffing decisions are a matter for the company concerned. However, given the importance of platform security, the PSA's expectation is that all platform providers have adequate resource, either internal or externally contracted, focused on security and fraud. The PSA recommends that security staff should be able to meet the following competencies:

- ability to evaluate risks in platforms and software and research security incidents
- good understanding of web security and internet security tools
- understanding of threat modelling.

The PSA's expectation under Code Requirement 3.10.1 is that all platform providers have an assigned Head of Security or other equivalent senior role. The PSA recommends that a Head of Security or equivalent senior person should be able to meet these competencies:

- demonstrable knowledge of the latest security thinking and threat modelling methods
- ability to manage complex IT platform overhaul projects, if required
- significant knowledge and experience of IT/web security to enable the effective identification, management and control of security and fraud risks
- significant knowledge and experience of security management systems and processes.

Where such a role is vacant as a result of staff departure or absence, then responsibility should shift upwards to a more senior member of staff.

Each intermediary platform provider must have a nominated Single Point of Contact (SPoC) whose details have been shared with the PSA via the PSA Registration System (Code Requirement 3.10.2), the connecting network(s) and any relevant industry stakeholders. This is so that if an incident does occur, no time is wasted in investigating and rectifying issues.

We recommend that all relevant providers ensure that platform development staff are trained in secure development techniques and have an understanding of relevant risks and threats to an appropriate level. Training should be undertaken periodically, to take account of threat and risk evolution and to keep skills current.

Our expectation is that all platform development staff should build their understanding of relevant risks and threats into any development work they carry out. Relevant providers will be expected to be able to demonstrate this on request by the PSA.

The PSA's expectation is that all platform or other systems development – including but not limited to new protocols for phone-payments – should have their functionality reviewed by the provider's security team before they go live.

The PSA recommends that the Head of Security (or equivalent senior person) should have the authority to veto any protocols or solutions and ensure that any systems changes are not implemented without an audited assessment and approval from the security team. Where the decision is taken not to follow this recommendation, the provider should be able to demonstrate how they achieve an equivalent level of assurance. An example of template for recording such an assessment is attached at Appendix B. The use of this template is voluntary and is intended to set out the level of detail the PSA would expect to receive about assessments where relevant to an investigation.

Appendix A – Glossary of technical terms

Attacker behaviour analytics - where web and payment platforms analyse previously known patterns of cyber-attacker behaviour and use the trends in that data to identify repeats of those attacks, or the next potential variants of those attacks.

Authentication cookies - the most common method used by web servers to know whether the user is logged in or not, and which account they are logged in with. A cookie is a small piece of data sent from a website and stored on the user's device by the user's web browser while the user is browsing. This is usually to remember information, such as any items a user has added to a shopping cart, or to record the user's browsing activity (including clicking particular buttons, logging in, or recording which pages were visited). They can also be used to remember information that the user previously entered into form fields such as names, addresses, passwords, and card details or phone numbers for payment.

Content Security Policy (CSP) - a computer security standard introduced to prevent various types of attacks where malicious code is injected into a trusted web page. CSP works by providing a standard method for website owners to declare approved origins of content that browsers should be allowed to load on that website. Anything which is not approved cannot be loaded.

Coordinated vulnerability disclosure scheme - a scheme established to enable network operators and/or intermediary providers to work cooperatively with security researchers and other relevant persons to find solutions to remove or reduce any risks associated with an identified vulnerability in their services and/or systems. Such a scheme involves the reporting of vulnerabilities to network operators and/or intermediary providers by security researchers, and the coordination and publishing of information about a vulnerability and its resolution. The aims of vulnerability disclosure within such a scheme include ensuring that identified vulnerabilities are addressed in a timely manner; removing or minimizing any risks from any identified vulnerabilities; and providing users with sufficient information to evaluate any risks arising from vulnerabilities to their systems.

Council for Registered Ethical Security Testers (CREST) - an international not-for-profit accreditation and certification body that represents and supports the technical information security market. CREST provide internationally recognised accreditations for organisations, and professional-level certifications for individuals providing various types of cyber-security services.

Cross-Site Scripting (XSS) - a type of computer security vulnerability which typically exploits known vulnerabilities in web-based applications, their servers, or the plug-in systems in which they rely. An attacker "injects" malicious coding into the content being delivered by the web application. When the resulting "combined" content arrives at the user's web browser, it has all been delivered from the trusted source, and thus operates under the permissions granted to that system.

Common Vulnerability Scoring System (CVSS) - a free and open industry standard for assessing the severity of computer system security vulnerabilities, created following research by the US National Infrastructure Advisory Council in 2003/04. Vulnerabilities are rated on a scale of one to ten, with ten being the most severe.

Hyper Text Transfer Protocol (HTTP) - the underlying protocol used by the World Wide Web, which defines how messages are formatted and transmitted, and what actions web servers and browsers should take in response to various commands.

Hyper Text Transfer Protocol Secure (HTTPS) - the secure version of HTTP. HTTPS is encrypted in order to increase security of data transfer. This is particularly important when users transmit sensitive data

HTTP Strict Transport Security (HSTS) - a web security policy mechanism that allows web servers to declare that web browsers (or other complying user agents) should interact with it using only secure (HTTPS) connections, and never via the insecure HTTP protocol. A website using HSTS must never accept clear text HTTP and either not connect over HTTP or systematically redirect users to HTTPS.

Mobile Origination message (MO) - a text message which has been originated on, and sent from, a mobile device. These can be either free – i.e., the cost of sending the message is that of sending a standard text – or charged at a premium when the text is received by the mobile shortcode to which it was sent.

Mobile Termination message (MT) - a text message which is received by a mobile device. These can either be free – i.e., receiving the message costs the recipient nothing – or charged at a premium when the device receives the message. In the context of phone payment, MT messages are usually generated by a Level 1 provider in response to consumer interaction with a Level 2 provider merchant. Where they are not, it may be that the message and any associated charge was unsolicited.

National Cyber Security Centre (NCSC) - an organisation of the UK Government that provides advice and support for the public and private sector on how to avoid computer security threats. One of their products is the NCSC Cyber Security Essentials certification, a set of basic technical controls to help organisations protect themselves against common online security threats. Cyber Essentials is backed by industry including the Federation of Small Businesses, the Confederation of British Industry and a number of insurance organisations which are offering incentives for businesses. From 1 October 2014, the Government has required all suppliers bidding for contracts involving the handling of certain sensitive and personal information to be certified against the Cyber Essentials scheme.

Network internet provision - an Internet service provider (ISP) is an organisation that provides services for accessing, using, or participating on the Internet. Where a consumer uses the internet access provided by their network to browse the web with their device, this is known as "Network IP".

Open Web Security Application Project (OWASP) - a worldwide not-for-profit charitable organisation focused on improving the security of software, so that individuals and organisations are able to make informed decisions. Operating as a community of like-minded professionals, OWASP issues free, open-source software tools and knowledge-based documentation on application security. The *OWASP Top 10* is a project to document the ten most critical categories of security risk to web applications. It represents a broad consensus of a variety of security experts from around the world, who share their expertise to revise the list on a regular basis.

Payload protection -the payload is any message sent by a user's device to a website or other web application, where that message contains, or has had added, malicious coding. Payload protection is anyaction or system which seeks to identify and block messages containing malware.

Personal Identification Number (PIN) - a numeric or alpha-numeric password used to authenticate a user so they can access a website, web application, or any other system.

Rate limiting - is used to control the rate of traffic sent or received by a network interface controller. In the context of phone payment, it prevents repeated attempts by an attacker to send the same message or execute the same action. A common example is the rapid and sequential entry of every possible four-digit PIN until the correct one is entered, thus allowing an attacker who does not know the PIN to gain access through repetition.

Red team/blue team testing – is *w*here a security function divides into two teams in order to conduct penetration testing. One, the Red Team, uses malware the team has discovered to try and execute that malwareon a "sand boxed" version of the platform, with the Blue Team attempting to identify and prevent any attempts.

Threats - known malicious indicators that appear together during specific cyber-attacks. By recording and aggregating intelligence about threats, payment platforms and web applications can identify and prevent further attacks using the same methods and look to predict what variations on previous attacks may appear next.

Transport Layer Security (TLS) - an encryption protocol that protects data when it moves between computers or other devices. When two devices send data, they agree to encrypt the information in a waythey both understand. This prevents data being intercepted by a third party, or "injected" with malicious code.

Time delta - where a user interacts with a website or web application, and in particular where they click on-screen buttons, the time delta between clicks is an important way of ascertaining whether the interaction is genuine or is potentially being carried out by a device infected with malicious code. Sometimes an infected device will "click" more rapidly than a human being could or will click on the exact same pixel within a sequence of buttons which are presented.

Uniform Resource Locator (URL) - the formal term for a web address.

X-header request - the instruction sent by a device in order to "pull" a specific website or webpage to it and display the page so a user can browse it. In effect, the X-header request ID correlates the HTTP request between a user's device and the website or web application's server.

Appendix B – Example templates for security records

Assessment of New Platform or Systems Developments

<table>
<tr><td><b>Description of the proposed update/new protocol/development</b></td><td colspan="4"></td></tr>
<tr><td><b>Person(s) responsible for security assessment</b></td><td colspan="4"></td></tr>
<tr><td><b>Summary of the security assessment (e.g., methodology used to assess and test)</b></td><td colspan="4"></td></tr>
<tr><td><b>Pass or fail?</b></td><td colspan="4"></td></tr>
<tr><td rowspan="4"><i>If “pass”, were there any dissenting views?
Please provide details</i></td><td><i>Person(s) who dissented</i></td><td colspan="2"><i>Reasons for dissent</i></td><td><i>Relevant OWASP category</i></td></tr>
<tr><td></td><td colspan="2"></td><td></td></tr>
<tr><td></td><td colspan="2"></td><td></td></tr>
<tr><td></td><td colspan="2"></td><td></td></tr>
<tr><td rowspan="4"><i>If “fail” please provide details of the reasons for failure</i></td><td colspan="2"><i>Description of the identified issue/weakness/risk</i></td><td colspan="2"><i>Relevant OWASP category</i></td></tr>
<tr><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td><b>Will the proposal be re-submitted?</b></td><td colspan="4"></td></tr>
<tr><td rowspan="4"><i>If it will, what improvement actions are required?</i></td><td><i>Description of the action</i></td><td><i>Who is responsible for the action?</i></td><td><i>Date the action is assessed as complete</i></td><td><i>Who signed it off as complete?</i></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>

Record of identified security incident

Description of identified breach or attempted attack	*Breach or attempted attack?*	*Description*	*Relevant OWASP category*	
When and how was it identified?	*Date*	*Time*	*How was it flagged?*	*Who was the SPoC?*
Person(s) who performed the initial assessment				
Summary of the incident and the SPoC's assessment				
Was the incident reported to?				
MNOs?	*Date and time*	*Person reporting*	*Summary of further/ongoing actions that resulted*	
PSA?	*Date and time*	*Person reporting*	*Summary of further/ongoing actions that resulted*	
ICO?	*Date and time*	*Person reporting*	*Summary of further/ongoing actions that resulted*	
What immediate actions were required?	*Summary of action*	*Who is responsible for the action?*	*When was the action completed? (Date and time)*	*Who signed the action off as complete?*
What remedial actions were required?	*Summary of action*	*Who is responsible for the action?*	*When was the action completed? (Date and time)*	*Who signed the action off as complete?*