Smart Card Web Server, How to bring operators' applications and services to the mass market

February 2009

Executive Summary

From the earliest beginnings of mobile communication, the SIM card has been a key component in the telecoms market, ensuring user authentication on operators' networks. It is today the only physical link between operators and their customers.

Since its introduction, the SIM card has evolved from simple user authentication to become a services platform for operators to run applications such as phonebook synchronisation or S@T menus, enhancing the discovery and usage of operator services.

But now, as mobile applications and services are becoming more and more sophisticated, thanks to the evolution of the mobile handset, it is time for the SIM card to move to its next phase and introduce a brand new technology: the **Smart Card Web Server (SCWS).**

The SCWS is a new environment in which to develop, execute and distribute content rich applications from the SIM, based on web technologies. It aims to offer operators a new approach to enhance the usage of their key services by the mass market.

The SCWS constitutes the **new trend in the evolution of Smart Card** technology. First, the SCWS provides a **next generation user interface** for the end-user, moving from black and white menus to rich a web "look and feel" for its applications. Then, as it is based on Internet languages, the SCWS **makes the development** of SIM-based applications easier, while facilitating **their distribution**. Also, the SCWS **enhances connectivity with remote web servers** to enable client/server applications to take full advantage of the evolution in network speeds.
After many years of development and standardization efforts, and with the first handsets now hitting the market, the SCWS is ready to open up a new era for SIM-based Internet applications.

The **SIMalliance's strategy** for accelerating the growth of this business area includes the promotion of a comprehensive and shared vision of the SCWS technology and its benefits for the mobile industry.

In this White Paper, the SIMalliance analyzes **SCWS's positioning** in the telecoms ecosystem, from marketing considerations such as its unique benefits and the use cases it could enable, to a detailed overview and discussion surrounding its implementation and associated standards.

The Paper aims to provide ecosystem players, particularly Mobile Network Operators (MNOs) and Service Providers (SPs), with a common understanding of such new functionalities. It also provides detailed information that will help them evaluate the opportunities, develop their markets and promote their participation in the ecosystem.

Table of Contents

Smart Card Web Server at A Glance

The **Smart Card Web Server (SCWS)** is the new generation of SIM application environment in which to develop rich services on the SIM without any prior customization of the handset to perform.

As every operator's customer owns a SIM, this means that any application developed using the SCWS technology could reach any end-user, whatever their device, opening up a new mass market distribution channel for operators' applications.

The SCWS is based on a standard **HTTP 1.1 web server embedded in a smart card,** allowing communication with any HTTP client - particularly the handset browser that will be used as a powerful user interface for services and applications.

Moreover, any SCWS-related applications and associated content can be managed remotely by an administration server. As a consequence, the SIM card can be customised "over the air" to provide up-to-date applications/content to fit to the expectations of any user.

Smart Card Web Server Benefits

Compared with current solutions implemented on the handset, the **Smart Card Web Server (SCWS)** provides a number of unique advantages such as:

Easier service & application development and deployment

Thanks to the smart card's interoperability, a SCWS-based application is a build-once, deploy to all solution suitable for handsets**, no matter what the handset's operating system or handset middleware is. It will support MAC OSX™, Android™, Linux, Symbian™, Microsoft Mobile™ and even native OS, in addition to any handset middleware, such as Qualcomm BREW and SUN JavaME™.

The time-to-market to deploy a SCWS-based solution is shortened by concentrating efforts on a single element. The whole SCWS-based application can be installed and personalized using the current smart card supply chain. In addition, transparent post-issuance updates can be performed using remote administration servers to download new content or applications.

The content of the smart card is perfectly controlled. The service provider is assured that its service can be installed, updated or removed at any time and only by the authorized entity. This solves the main issue of deploying applications in an uncontrolled environment such as a handset, where problems such as the accidental deletion of a critical application by the end-user may occur.

Service and user-experience continuity

SCWS-based solutions improve the portability of applications and services in cases of handset renewal; there is no need to reload user applications, while only a slight rendering is needed to adapt the content to handset screen size. This is performed remotely and transparently for the end-user.

In addition, the provider can rely on service continuity while providing the same user experience, either online or offline. This will also increase familiarity with the mobile internet user environment to encouraging increasing adoption by end-users. Moreover,
user preferences could be stored securely and transported from one handset to another.

Security

SCWS implements, in a tamper-proof device, security between all the nodes of its ecosystem. From the security of data at the transport level with OMA standards (PSK TLS), to the implementation of GlobalPlatform standards to ensure security at application level, SCWS provides operators and third parties (and particularly banks) with the secure environment they need for their applications.

A real execution environment

Thanks to the legacy of SIM Toolkit, the SCWS acts as a real-time execution environment for applications and provides handset APIs to:

- intercept incoming calls and SMS
- initiate outgoing calls and send SMS
- retrieve location information (cell ids, roaming, visited networks...)
- retrieve data from the cloud (in the background and invisibly for the end-user)

***some slight adaptations may be required*

- provide secured local storage for client/server applications (search history, last updates…)
- provide access to SIM phonebook
- launch browser based on various events
- detect handset model to adapt content to screen size

A future-proof technology

Leveraging the handset browser, the Smart Carc Web Server (SCWS) will benefit from all the latest improvements of this particular client (JavaScript, XMLHttpRequest) to enhance the user experience and the performance of local applications. And critically, the SCWS supports browser plug-ins such as Adobe Flash or SVG-Tiny to bring applications' user interface to their next level.

What Applications for Smart Card Web Server?

The **Smart Card Web Server (SCWS)** offers operators and developers a powerful execution environment, combining the advantages of local runtimes (access to device APIs, local storage) and web languages (easy development, ability to retrieve data from the internet).

Also, for end-users this means that SIM-based applications will get an interface fully in line with their expectations, even on high-end handsets.

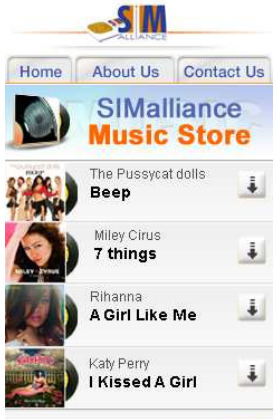
This section describes details of applications that could be developed in vertical segments according to operators' needs:

Service and content discovery

In the mobile world, most end-users are not fully aware of all value-added services offered by their Operator or Service Provider (WAP, SMS Premium, IVR services). Today's mobile experience requires consumers pay to view operators' WAP services, while slow connection times and a complex user experience provide little incentive. Even though the situation is improving with the arrival of high-speed broadband Internet (and flat rate data charges), most users are still not using operators' key services, unaware of the benefits.

Utilising a regular handset browser, the SCWS can provide a set of offline web pages allowing end-users to discover at anytime, anywhere and free of charge, the operator's 'preferred' services. This will drive the adoption of the mobile web environment and increase end-user loyalty and confidence to explore operators' online services.

Catalogues



The mix between local and remote content can be optimized to favour the online purchase of music, videos, games or any other multimedia content. For example, the content stored in the smart card provides a local catalogue of content with a rich display, where the end-user can preview and listen before buying. This content could be updated on a periodical basis to encourage further use of these services.

The same principle could also be applied to create an operator application store to promote its handset clients and allow their download.

Operator Wizards

The SCWS could be used to develop various wizards to accompany users in their mobile journey:

- ***Welcome Screen***: using the launch browser command, the SCWS could display at handset power-on an operator menu welcoming subscribers to the operator network,

providing them with guidance on how to use the operators' services or helping them to configure their handset.

- ***Interactive Helpdesk***: using the call interception function combined with the launch browser command, the **Smart Card Web Server (SCWS)** could intercept calls to the hotline and provide a first level of helpdesk to end-users. This could range from a simple text-based resolution of an issue up to configuration of the handset by a device management platform based on the SCWS inputs. That way, operators could reduce their hotline costs and differentiate themselves from the competition

- ***Self-Care***: in order to make it easier to check the balance of subscribers' accounts (Voice Minutes, remaining SMS) and to top-up their accounts, the SCWS could be used to provide a self-care interface to facilitate the management of subscribers' accounts and to boost top-up usage. Moreover, leveraging the naturally high traffic for this kind of operation from both post-paid and pre-paid subscribers, it could be a good way to drive additional online traffic by the cross-marketing of additional operator services at the same time.

Communication clients

As mobile Internet is now coming to the market, IP communication services such as Instant Messaging, E-mailing or even Micro-Blogging are now starting to find their place in the mobile environment and provide the potential for growth in operators' communication revenues. Unfortunately, to make them available for the mass market, the applications have to be developed on multiple handset environments and then preloaded on the various handsets, a complex and costly process.

Thanks to the SCWS and without any pre-configuration of the handset, it is now possible to redesign these clients on the SCWS runtime engine and facilitate their distribution to the mass market with a rich, graphical user interface.

Making contactless technology a consumer service

Contactless technology enables mobile phones to be used for transport access, payments, ticketing and many other proximity services. Local contactless connectivity and related applications can be managed by a secure element such as a smart card. Key improvements coming from the SCWS are:

- There is no need to deploy client applications on terminals to enable a contactless service user interface. All interfaces are embedded in a single secure element.
- The user interface provides the same user experience in any contactless terminal.
- Access is fast and always on, with no application execution environment or network coverage required to start the application

- Security is improved as transactions are made directly between the server and the contactless secure element.

Advertising

Thanks to the advanced graphical interface, the Smart Card Web Server (SCWS) can host various Ad formats such as text-links or banners. Inserted in operators' applications and services, this could drive an additional revenue stream from advertising.

Handset client configuration using the SCWS

On top of the generic usage in correlation with the handset browser, the SCWS could be used to communicate with other handset applications to configure them. For example, resources of an agent such as the HomeScreen could be hosted on the SCWS to allow a customisation of the HomeScreen at handset power-on. That way, the look and feel of the idle screen could be adapted to the operator's branding.

Other applications

The applications listed above are just examples of what could be developed using SCWS technology however it is certainly not exhaustive. The market needs now to adapt this technology to their needs and what services can be brought to the mass market is only limited by imagination!

Smart Card Web Server: Technical Overview

How does Smart Card Web Server (SCWS) browsing work?

SCWS browsing

The SCWS is an application residing in the smart card which **implements a HTTP 1.1 server**. The SCWS content is accessible just by selecting on the Internet browser an **URL pointing on the smart card**.

The selected URL can provide **static resources** such as xHTML files, images, multimedia files or any file format managed by the HTTP client such as the Internet browser. The URL can also be handled by a **web application** installed in the card in order to perform some specific tasks or to ***dynamically*** generate an xHTML page.

The SCWS can provide **any content** as long as this content can be managed by the Internet browser. If rendering issues exist on the device, they can be solved either by the web application in the card or remotely by downloading appropriate content fitting the handset in the card.

Security

The SCWS provides several mechanisms to secure the HTTP connection:

- User authentication mechanisms as defined by HTTP
- Authentication and confidentiality with the implementation of HTTP over TLS (HTTPs)
- Control of the access to the SCWS from device applications by using the Access Control Policy (ACP) defined in the OMA specifications

How does Smart Card Web Server (SCWS) remote management work?

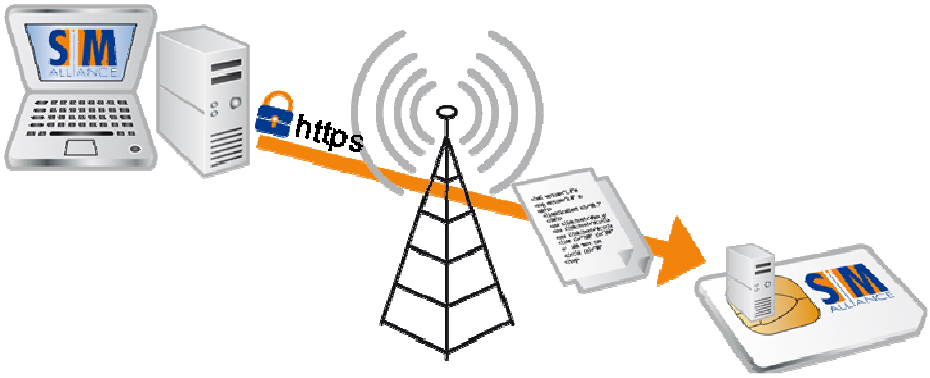
The SCWS and its servlets can be managed remotely, to modify, add to or adapt their contents.

For these dynamic management purposes a new protocol has been defined and standardised at OMA, to open a secure pipeline between the SCWS in the card and the Over-The-Air platform:

- remote management of SCWS local pages
- any secure interaction between the card and a telecom operator server

The main characteristics of this protocol are:

- The card is seen as a client
- The OTA platform is seen as a server
- The card communicates with the OTA platform using web protocols (HTTPS)
- The Security layer is “Transport Layer Security” (the “S” in HTTPS), in a “Pre-Shared Key” mode
- Part of the intelligence is switched to the client (retry management, for instance)



How do Smart Card Web Server web applications work?

In order to provide dynamic content, the SCWS web applications can be installed in the smart card. When the Internet browser requests an URL mapped to a web application, the application is triggered and generates the xHTML page dynamically.

As the whole application is stored in the smart card, SCWS web applications can be easily and efficiently deployed during the card personalisation process, reusing the current smart card supply chain process. The SCWS web applications can be downloaded or updated remotely using the Remote Application Management specification defined by GlobalPlatform, once the smart card has been issued.

ETSI specifications provide the framework and the Application Programming Interface (API) to implement SCWS web applications for Java Card ™ 2.2 platforms.

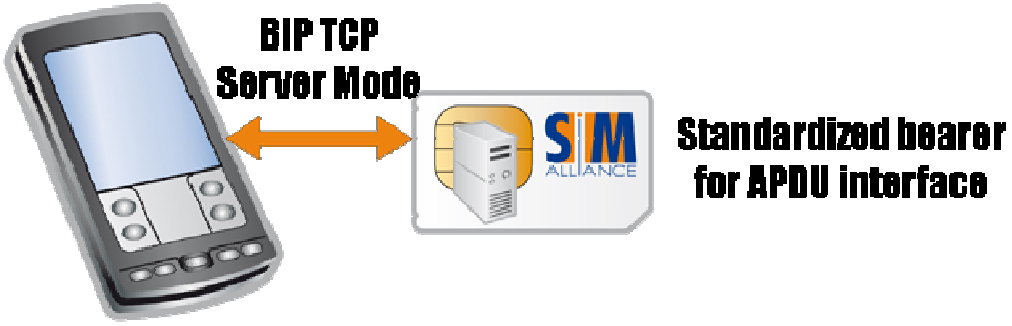
The GlobalPlatform specifications include the management of web applications for Java Card ™ 2.2.

The OMA, ETSI and GlobalPlatform specifications, associated test specifications and SIMalliance guidelines provide a high level of interoperability for the SCWS solution.

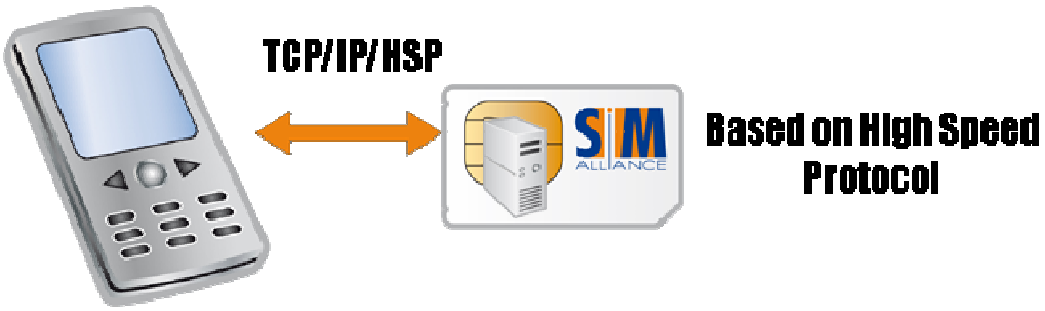
SIM Cards supporting Smart Card Web Server

There are two categories of cards supporting **Smart Card Web Server (SCWS)**:

- Classic ISO cards (up to a few MB), communicating using BIP TCP server mode with the handset



- USB-IC cards (up to GB), leveraging high speed communication protocols and that could either communicate with the handset supporting BIP TCP server mode or TCP/IP.



The SCWS can be used with BIP (Bearer Independent Protocol) over the ISO 7816 interface or with a full TCP/IP stack over the New UICC-Terminal interface USB.

There is still a migration phase ahead of us to move from the legacy ISO to the USB interface which will be supported by the handsets in the near future.

As a first step, with the present handset implementation of BIP in server mode and the legacy ISO interface in the SCWS enabled UICCs, it is already possible to benefit from the next generation UICC services that are offered by the SCWS.

As soon as there are more USB-enabled handsets available, the whole system can profit from a more convenient communication speed, however BIP communication over ISO already provides a good user experience for most of the potential uses described before.

In the future, there will also be a transition from the JavaCard 2.2 to the JavaCard 3.0 operating system. Although the new JavaCard 3.0 specifications have been designed around the SCWS to help the development of web applications, many features and functions are already already covered by the Java Card™ 2.2 standard to enable most of the use cases.

Devices that could host a Smart Card Web Server-based solution

Mobile handsets are, of course, the first targeted devices for **Smart Card Web Server (SCWS)**-based solutions. Most handsets are already integrating the Bearer Independent Protocol (BIP) over ISO in client mode.

In order to manage the SCWS, handsets just have to integrate a software layer implementing the server mode. This functionality allows the card to ask the handset to open a TCP port on a local address and then to behave like a server.

In the future when handsets will manage a full TCP/IP connection, the SCWS will be automatically reachable using the card IP address.

One should note that a SCWS-based solution can be easily integrated into any other device, eg laptops, using a smart card implementing a TCP/IP connection.

LG has been the first handset provider to implement BIP TCP server mode in its handsets. Many other handset providers are already supporting these functionalities and for handset manufacturers, 2009 will be Year One for the commercial availability of such products.

Applicable Specifications for SCWS-based Solutions

The **Smart Card Web Server (SCWS)** technology is standardised by the Open Mobile Alliance (OMA). The OMA SCWS v1.0 enabler defines an HTTP 1.1 server embedded in a smart card, the URL used to access the card content. An administration protocol is also defined, allowing the update of the SCWS content and configuration remotely. This full administration protocol is also based on HTTP 1.1. OMA defines a new release of the SCWS: the SCWS v1.1 enabler. This new release includes a set of optimisations of the SCWS 1.0 enabler. The remote management of the SCWS from different trusted entities is optimised, each entity being able to control what content and which smart card applications can be accessed under a given URL. The SCWS v1.1 also improves the efficiency of the exchanges with the HTTP client in the terminal.

In order to develop interoperable SCWS applications providing dynamic content, ETSI SCP (Smart Card Platform) has defined an API available for the Java Card ™ Platform. This API allows HTTP requests to be forwarded to an applet and then the response of the applet to be sent back.

Finally, GlobalPlatform defines a remote administration protocol to administrate the dynamic content application. This protocol is fully compliant with the remote administration protocol defined by OMA to administrate the static content.

Specifications		Location
OMA SCWS v1.0 enabler	SCWS v1.0 Architecture SCWS v1.0 Technical Specification	http://www.openmobilealliance.org/Technical/release_program/SCWS_v1_0.aspx
OMA SCWS v1.1 enabler	SCWS v1.1 Technical Specification	http://www.openmobilealliance.org/Technical/release_program/SCWS_v1_1.aspx
ETSI TS 102 588 Release 7 and higher Smart Cards Application invocation Application Programming Interface (API) by a UICC web server for Java Card™ platform	API to implement SCWS web applications	www.etsi.org
ETSI TS 102 223 Release 7 and higher Smart Cards Card Application Toolkit (CAT)	Specification of the BIP protocol in client mode (Class 'E' defined in Release 4 and beyond), and in server mode (defined in Release 7 and beyond)	www.etsi.org
GlobalPlatform Card Remote Application Management over HTTP Card Specification v 2.2 - Amendment B	Remote management of applications over HTTP	www.globalplatform.org
Java Card™ 2.2.1	Java Card™ Specifications	www.java.sun.com

Specifications		Location
- Virtual Machine Specification - Runtime Environment (JCRE) Specification - Application Programming Interface		
ETSI TS 102 241 Smart cards UICC Application Programming Interface (UICC API) for Java Card™	Java Card™ 2.2.1Toolkit API	www.etsi.org
ETSI TS 102 221 Release 7 Smart Card UICC-Terminal Interface: Physical and Logical characteristics	UICC physical and logical characteristics	www.etsi.org
ETSI TS 102 483 Release 7 Smart cards UICC-Terminal interface; Internet Protocol connectivity between UICC and terminal	IP connectivity to allow direct connection of TCP/IP over HSP	www.etsi.org
ETSI TS 102 600 Release 7 Smart Cards UICC-Terminal interface; Characteristics of the USB interface	High Speed Protocol (HSP) specification based on USB IC	www.etsi.org

Interoperability and SIMalliance

Since its foundation, the SIMalliance has worked closely with key participants in the mobile services ecosystem to ensure interoperability between SIM, handset and OTA platform. This has been demonstrated through a number of technical documents, tools and test workshops created by the SIMalliance itself or in co-operation with other bodies.

To ensure interoperability for the **Smart Card Web Server (SCWS)**, SIMalliance's members have participated in several dedicated interoperability testing events since 2007, including OMA SCWS 1.0. During this test, OMA SCWS 1.0 specification has been successfully approved, while testing the interoperability of the ecosystem with different implementations of cards, handsets and servers.

SIMalliance members have been supporting standardisation bodies such as OMA (Open Mobile Alliance) and ETSI SCP (Smart Card Platform) who not only have worked closely together in order to create the relevant primary standards but also to develop the related test specifications which allow the correct implementation of these standards.

Beyond the inter-working of external interfaces between smart cards, terminals and remote servers to applications on the UICC, ETSI SCP also created a specification of an API for the UICC-based SCWS, defined by OMA.

Conclusion: Smart Card Web Server, a bright future

Thanks to the **Smart Card Web Server (SCWS)**, a new generation of SIM-based applications is now ready to hit the market. SIMalliance members consider the SCWS as the central enabler to bring web services to the SIM card. Operators now have a new technology to develop their advanced applications on the smart card while reducing their overall customisation effort.

The basis for the success of the SCWS is at hand as the technology is now ready:

- Standards have been created
- OMA Test have been performed
- Implementations for handsets and cards are available

The SCWS is ready to go. A new era for SIM-based Internet applications is at the door.

The market demand is developing

2009 will be Year One for Smart Card Web Server!

Glossary

BIP – Bearer Independent Protocol: Technology, standardised at ETSI, based on TCP/IP, allowing the SIM card to communicate efficiently with the handset and the network.
ETSI – European Telecommunications Standards Institute http://etsi.org/
GP – GlobalPlatform http://globalplatform.org/
HTTP – Hypertext Transfer Protocol: a communications protocol for the transfer of information on the internet. HTTP development was coordinated by the World Wide Web Consortium and the Internet Engineering Task Force (IETF).
HTTPs – A short term for HTTP over TLS.
Java™ – A network-oriented programming language invented by Sun Microsystems. Java was specifically designed so that programmes could be safely downloaded to remote devices (e.g., web pages). Java is a registered trademark of Sun Microsystems Inc.
OMA – Open Mobile Alliance http://www.openmobilealliance.org/
OTA – Over-The-Air: Transmission using microwave channels. This acronym is used in the world of wireless telecommunications.
SIM – Subscriber Identity Module - A smart card for GSM systems holding the subscriber's ID number, security information and memory for a personal directory of numbers, thus allowing him to call from any GSM device. It can also store and run applications enabling end-user services.
SIM Toolkit – A data management application for SIM cards, part of which is resident in the SIM card
Smart Card – Also called IC card, chip card or memory card (for certain types). A card formed of a plastic body with a chip (or module) embedded in a special cavity.
SCWS –- Smart Card Web Server. Technology standardised at OMA that enables the embedding of a web server in a SIM card.
SMS – Short Message Service, or text message, is a service that sends and receives messages of up to 160 characters to and from a mobile phone. It can also be used as a bearer for data applications.
TCP-IP – Transmission Control Protocol / Internet Protocol Communication protocols forming the basis of the internet.
TLS – Transport Layer Security that provides secure communications on the Internet
UICC –Universal Integrated Circuit Card as defined by ETSI TS 102 221 www.etsi.org
USB-IC – USB Inter-Chip: high speed protocol.
WAP – Wireless Application Protocol
Web page – A document viewable by using a web browser or client application which is connected to the page server
Web server – A server process running on a processor, which sends out web pages in response to HTTP requests from browsers.
wHTML – Wireless Markup Language. The cornerstone of WAP, WML is based on XML. It is a standard technology for creating web pages on the internet. WML pages can be stored on standard internet servers.
xHTML – eXtensible Hyper Text Markup Language. Replacement markup language for HTML. XHTML is similar to HTML, but is designed to work with the XML, the core language for designing web applications.